Georg Philip Krog og Anne Gunn B. Bekken (red.)

YULEX 2004

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 82-7226-083-2
ISSN 0806-1912

unipubskriftserier

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

Institutt for rettsinformatikks utgivelser i skriftserien Complex er støttet av:
Advokatfirmaet Selmer DA
Wikborg Rein & Co
Lovdata

FORORD

Denne boken er den fjerde i Yulex-serien.

Siktemålet med serien er å tilby venner av Institutt for rettsinformatikk smakebiter fra ulike temaer som har opptatt instituttets medarbeidere i løpet av dette året.

De fleste av årets artikler har enten vært publisert eller fremført som foredrag i internasjonale fora.

Opplysninger om forfatterne er tilgjengelig på
http://www.jus.uio.no/iri/om_iri/folk/index.html

God jul og fornøyelig lesning!
Georg Philip Krog og Anne Gunn B. Bekken

PREFACE

This book is the fourth in the Yulex series. The aim with the series is to offer friends of the Norwegian Research Center for Computers and Law a "Christmas smorgasbord" of the various themes upon which Centre staff have been working over the past year.

Most of this years articles have either been published or presented in international fora.

Information about the authors is available at
http://www.jus.uio.no/iri/english/nrccl/people/index.html

Merry Christmas and happy reading!
Georg Philip Krog and Anne Gunn B. Bekken

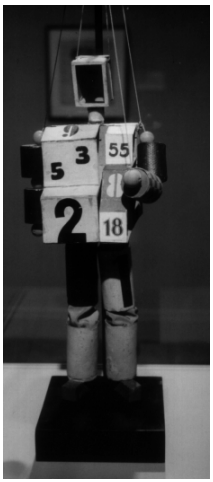
INNHOLDSFORTEGNELSE

1 THE RIDDLE OF THE ROBOTS[1]

By Jon Bing

1. The riddle

In 1993 I made a journey to Chicago, an excursion with some colleagues and graduate students to visit the Chicago-Kent School of Law and other institutions related with my own research area, computers and law. During the stay, we visited the Art Institute of Chicago. And there I made a remarkable discovery. In its collection I discovered a small three-dimensional figure made of cardboard.[2] The head is reminiscent of a cathode ray tube; the body is made up of boxes decorated with numbers, the feet are two tubes. Anybody would interpret this figure as a robot, and this is indeed the name of the artwork. The artist is Alexandra Alexandrovna Exter, and she made this small figure in 1925.



It was the date that puzzled me.

"Robot" is a rather recent word. It was used the first time by the Czech author Karel Čapek (1890-1938). Čapek was an important and profilic author, famous for his many novels and plays. Many have read *War with the Newts* (1936), which is a very funny and very serious science fiction novel ridiculing the emergence of the Nazi movement, and indicating Čapek's strong political involvement.

His play *R.U.R.,* which is an abbreviation for "Rossum's Universal Robots", is also of a political nature. In this play, the main character is Rossum, an industrialist who creates artificial beings from biological material in order

---

1 A written version of an invited talk to 'IRIS – Internationales Rechtsinformatik Symposium' at the Universität Salzburg, introducing the parallel session "Science Fiction and AI". There have been published versions of this in Norwegian, for instance "Dobbeltgjengere: Om maskinmennesker og menneskemaskiner i fantastisk litteratur", Jon Bing *Landskap med tegn,* Pax, Oslo 1998:89-106. I want to thank Associate Professor Dr Erich Schweighofer University of Vienna, Faculty of Law, Research Center for Computers and Law for giving me the opportunity to develop this English version.

2 The photograph is taken by one of the students, Viggo Elster, and has not been authorised by the Art Institute.

to have slaves in his production plants. There is a description of the process of building these beings:

'Spinning mills for weaving nerves and veins. Miles and miles of digestive tubes … in the fitting-shed, all the parts are put together like motorcars. They learn to speak, write and count. They have astonishing memories. But they never think of anything new. Then they are sorted out and distributed. Fifteen thousand daily, not counting a regular percentage of defective specimens which are thrown into the stamping-mill …'

It is maintained that the idea of such a play came to Čapek rather suddenly, and that he immediately discussed his idea with his brother Josef, who was a cubist painter.

"But," the author said, "I don't know what to call these artificial workers. I could call them Labori, but that strikes me as a bit bookish." "Then call them Robots," the painter muttered, brush in mouth, and went on painting. And that's how it was. Thus was the word Robot born; let this acknowledge its true creator.[3] *'*

The word 'robot' is derived from the Czech word 'robota', which means drudgery or 'servitude', and 'robotnik', who is a 'servant' or a 'serf'.

The play *R.U.R.* opened in Prague early 1921 and was extremely successful. It was produced in New York in 1922, and the English translation of the play was published in 1923.

Perhaps this is sufficient to explain what puzzled me with the figure of Alexandra Exter. For in Čapek's play, the robots are artificial human beings – they look exactly like humans, they would be what in modern science fiction jargon is known as an 'android' or a 'biomat', a machinelike man. But 'robot' is reserved for something different, for a mechanical man or a manlike machine, an artificial being built of hardware.

The word was created in 1921. Today it has a different meaning from what it originally intended. Somewhere along the line the meaning changed from 'machinelike man' to 'manlike machine'. And that point in time would seem to be located between 1921 and 1925 – because the figure of Exter is obviously that of a 'manlike machine', a robot in the modern sense of the word.

---

[3] http://capek.misto.cz/english/robot.html.

I admit it is a little mystery. But my own preoccupation with science fiction,[4] artificial intelligence and robots made this an intriguing one. And this essay is an explanation of the mystery.

2. Prague, ČAPEK and the Golem

It cannot be a coincidence that Čapek wrote his play about the artificial slave workers in the city of Prague. The famous Jewish ghetto of Prague is symbolised by the Golem.

A Golem is an artificial being, created by Man from earth and clay. It is said to be mentioned in Psalm 139:15-16:

'My bones were not hidden from you,
When I was being made in secret,
Fashioned as in the depths of the earth;
Your eyes foresaw my actions;
In your book all are written down;
My days were shaped, before one came to be.'

The 'depths of the earth' is a metaphor for the womb, emphasising the mysterious operations occurring there. And legend tells that at the end of the 16th century, rabbi Judah Löw followed the secret formula and fashioned in secret an artificial being from clay dug out of the banks of the river, and gave him life by placing a "Schem" – a capsule containing piece of paper with a cabbalistic word – in the mouth of the giant.

Rabbi Judah Löw, called The High Rabbi Löw because he was unusually tall, is a real person (1520-1609), his full name was Jehuda Liva ben Becalel. He was an acknowledged theological scholar, and shared his time between Prague and Krakow in Poland. In Pra-Prague, he founded the Talmud school Klause, part of the ghet-

[4] I have with Tor Åge Bringsværd edited a science fiction anthology with stories about robots, Jeg – en maskin, Gyldendal, Oslo1973.)

to. His grave can be seen in the cemetery, and still today one may find leaves weighted down by pebbles on his gravestone, he is believed to be a powerful rabbi whose spirit can be called upon for intercession.

The ghetto was the part of town in which the Jews were permitted to live. The living space was cramped, the lodgings small, the ghetto crowded. But it was generally believed to be very rich, as the Jews were successful business people. And there was considerable tension between the Jews and the rest of the population in the city – it was rumoured, for instance, that Jews ate babies in their un-Christian rituals, especially at Easter. The Golem was created by rabbi Löw as a defender of the ghetto, and over time the Golem became the symbol of the spirit of the Ghetto, like it appears in the well known novel *The Golem* by Gustav Meyrink (1868-1932). Meyrink was another Czech author living in Prague, and his novel was published in 1915, a few years predating Čapek's *R.U.R.* Still today clay figurines and other trinkets representing the Golem are popular souvenirs sold in the Ghetto. And the tale of the Golem still continues to fascinate writers, one of the more recent demonstrations is Marge Piercy *He, She, and It* (1991).[5]

In the original legend of the Golem, the artificial giant was somewhat simpleminded, taking all orders literally – in one episode, he does like the sorcerer's apprentice, when asked to fetch water, he continues to do so also even when the bowl overflows, and the house is flooded, the housekeeper having forgotten to ask him to stop.

Rumours of the giant reached the emperor Rudolph II of the Hapsburgs. His court must at this time have been a remarkable place, the emperor collected scholars and artists around him, and among them was another fascinating figure of that time, the astronomer Johannes Kepler. One may speculate on what form a dialogue between him and rabbi Löw would have taken, but we do not know whether they actually met.

It is said, however, that the court protocols of 22 February 1592 indicates that rabbi Löw was called to an audience before the emperor, with prince Bertier also present. The protocols do not tell what was said at this meeting, but leaving, rabbi Löw stated, 'We do not need Jossele Golem anymore.'

With this two friends and relatives Jakob Katz and Jakob Sosson, rabbi Löw takes the Golem to the chamber in the tower of the Altneu synagogue, which still stands at the edge of the ghetto. Here he reads a secret cabbalist formula over the Golem, reducing him once again to clay and dust.

It has been argued, even proved, that the tale of the Golem is much older than rabbi Löw, and that there are better candidates for his part in the story. 'Golem' shall also have been used in Jiddish for a simpleminded person, near-

---

[5] Published in Europe as *Body of Glass.*

nearly synonymous with a village idiot. This is of little concern in our context – the living tradition attributed the creation of the man of clay to rabbi Löw, and he became an obedient slave labourer.

As the novel of Meyrink demonstrates, the legend was very much alive at the time of Čapek. One of Čapek's acquaintances was the journalist Egon Erwin Kisch (1885-1948), who at that time worked in the German language newspaper *Bohemia* in Prague, writing local stories. Kisch would go on to become a famous reporter, earning himself the nick-name 'Der rasende Reporter' or 'The furious Reporter', especially due to his reports from the Spanish Civil War and other war theatres. His interest for the alleys and tales of Prague led him to write '*Dem Golem auf der Spur*',[6] where he traced the legend of rabbi Löw and his Golem. He entered the tower chamber of the Altneu synagogue and looked for the clay or dust remaining of the Golem, but without success.

Therefore, when Čapek conceived his idea of the industrialist Rossum and his artificial slave labourers, the Golem provided an obvious reference for his robots. But rather than creating them from clay and mystic rituals, Čapek let them be manufactured in vats similar to the chemicals provided for the factories of his own and modern age.

3. Frankenstein, his monster and the summer of 1816

However, this was not the first (nor the last, as we have seen) time that the tale of the Golem inspired the creation of an artificial being which since then has haunted our literature.

In 1816, the British poet Lord Byron (1788-1824) fled England due to rumours of his less than appropriate behaviour with respect to his half-sister. He fled in style, in a large horse-drawn carriage containing a library and a sleeping room, and he brought with him a social companion, a young man by the name of John Polidori (1795-1821), his father an Italian translating Gothic horror novels, himself a brilliant graduate from Edinburgh medical school. This background may not be wholly irrelevant, the medical school of Edinburgh was famous for its expertise in human anatomy, and expertise gained by dissecting corpses – and there were in the 18th century a brisk trade

---

6 Egon Erwin Kisch *Der rasende Reporter,* Aufbau Taschenbuch Verlag, Berlin 2001 (3rd edition). The original collection of essays was originally published 1925.

in corpses, graves in the city being robbed and its content sold to the University. This was sufficiently common for iron cages to be put on the graves to lock out the grave robbers.

Lord Byron's travels took him in the summer to Lac Lehman, where he rented a house, Villa Deodati (9 Chemin de Ruth, the house is still there) just outside the city of Geneva.

At the same time, another famous British poet also escaped to the Continent, Percy Bysshe Shelly (1792-1827). He had two years earlier eloped to the continent with the 17 year old Mary Godwin (1797-1851), the daughter of the philosopher William Godwin and the suffragette Mary Wollenstonecraft. Conveniently Shelley inherited a modest income and his wife, Harriet, committed suicide by drowning herself in the Serpentine, Hyde Park, leaving the two lovers free to marry and once more travel to the Continent.

Neither of the two spoke much French, but they brought with them Mary's step-sister, Claire Clairmont (1798-1879). She was an actress, and it is believed she had an affair with Lord Byron while she was performing at Dury Lane Theatre. She was still infatuated with him, and therefore it probably was not by chance that they came to rent Maison Chapuis, very close to Villa Deodati.

It is reported that it was a wet summer, robbing the two groups of the most obvious way of passing the time, making excursions into the splendid landscape. They had visitors, one of them was Matthew Lewis (1775-1818), one of the best known Gothic authors, his most famous book is *The Monk* (1796). He read aloud to them from the first volume of Göthe's *Faust* (1808) – Lewis translated the text from German as he read. The group also read aloud from other books, one of these was *Phantasmorgia,* a collection of Jewish folk tales which also included the legend of the Golem.

When reading about this summer and the persons staying at the shore of Lac Lehman, one is given the impression of a company of rather bored persons willing to experiment with intoxicating substances like belladonna in order to pass the time. And Lord Byron suggested that they should have a literary contest, each writing a Gothic tale. His own attempt was a less than successful attempt to write about a vampire, but which is recognised as the first literary vampire tale. It was just a fragment, Polidori came to publish his own story "The Vampyre" (1819) in such a way that it was attributed to Lord Byron, it is still disputed whether this was by design or accident.

The winner of the contest was, of course, Mary Wollenstonecraft Shelley, who published it as

Frankenstein – A Modern Prometheus (1818). The story has become part of our shared literary mythology, repeated and retold in numerous movies; the many trivial versions may overshadow the importance of the novel. One of the major themes of the novel is the moral responsibility of man – as God has moral responsibility for his creation, man, in the same way man has a moral responsibility for his own creation, in Frankenstein's case, the monster. The moral relations between a creator and the created is a theme that still is current, biotechnology making it perhaps more acute than in the time of Mary Shelley.

In the novel, the natural scientist Victor Frankenstein creates an artificial being by stitching together parts of corpses, and inducing life in these by sending the electrical power of a bolt of lightening into its nervous system. The Italian anatomist and physician Luigi Galvani (1737-1798) was one of the first to investigate experimentally the phenomenon of what came to be named 'bioelectrogenesis'. In a series of experiments started around 1780, Galvani, working at the University of Bologna, found that the electric current delivered by a Leyden jar or a rotating static electricity generator would cause the contraction of the muscles in the leg of a frog and many other animals, either by applying the charge to the muscle or to the nerve. Percy Bysshe Shelley was extremely fascinated by modern science, and this interest was shared by Mary, who in this way gives life to an artificial being using the methods of current science.

Frankenstein's monster is created using electricity, in Čapek's play the robots are created on some sort of assembly line in a chemical and industrial facility. The major difference is, perhaps, not the method of creation, but the fact that Frankenstein's monster is unique, while Rossum's robots are numerous, indicating a change of perspective from the moral responsibility of the individual to the political responsibility for a social order allowing the exploitation of the masses. In both cases, the artificial being is of flesh and blood, we have still to find the solution to the riddle of the robot.

4. Excursion: Ada Augusta, Lady of Lovelace and the Analytical Machine of Charles Babbage

A note should be permitted on another curious relation between the summer of 1816 and modern information technology. While staying in Villa Deodati, Byron worked on the third Canto of "Childe Herold's Pilgrimage", which the Shelley's and Clare Clairmont brought back with them to England while Byron continued his fateful journey.

This canto was dedicated to his infant daughter, Ada Augusta (1815-1852), who were to become Lady Lovelace. Ada Augusta had a talent for mathematics, and become the collaborator of the grumpy genius Charles Babbage (1791-1871), Professor at the Lucasian Chair of Mathematics at Cambridge (and famous for never giving a lecture to the students). He designed the Difference Engine, an advanced calculator, and the Analytical Engine – the latter in principle a general, mechanical computer using stacks of cogged wheels as a short-time memory and being programmed by the same punched cards used for Jaquard's looms.

The best description of this machine is notes of Lady Lovelace added to a translation of an essay published by the Italian engineer and mathematician Luigi Menabrea (1809-1896) in 1842 – Menabrea himself not being a minor figure, he became in 1867 Italian premier and foreign minister. It is through Lady Lovelace's notes we today retain the best discussion of the Analytical Machine, its construction, and the vision of how it could be programmed to solve any problem. Her insight has earned her the title of the world's first programmer.

In this way one may trace a thin thread of relation between the modern computer and the origin of Frankenstein's monster.

Perhaps of more relevance in our context, is one of the questions Lady Lovelace addressed – would the Analytical Machine be able to "think" in the sense that it would be able to create something novel. The question may be disturbingly modern, and is one also today haunting the research in artificial intelligence. Her answer, being known as Lady Lovelace's response, is that as the machine only could carry out the processes it had been programmed to do; it would not be able to do anything novel. This has later been challenged, perhaps most notably by Alan Turing (1912-1954) a century later, who emphasised that the machine could be programmed to learn from experience through feedback, and in this way might improve its own programs beyond the foresight of the programmer, and therefore arrive at results or behave in a manner not foreseen.

We may want to compare Lady Lovelace's response to the description of Rossum's robots, which is said not being able to "think of anything new". I have no reason to believe that Čapek was familiar with Lady Lovelace's notes, at his time, the work of Charles Babbage was regarded as a curiosity of no practical importance; Babbage's restoration only came after the construction of the first electronic computer, which in principle paralleled his Analytical Machine, and this realisation also brought fame to Lady Lovelace.

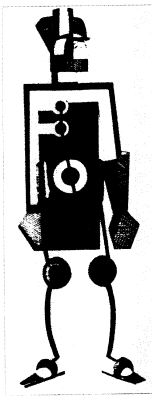
5. Alexandra Alexandrovna Exter and *Aelita*

Alexandra Alexandrovna Exter (originally Grigorovich, 1882-1949) was born in Bielostock, and attended art school in Kiev. In 1916, at a time when non-figurative art was still rare, Exter created her first totally abstract paintings. In the same year she began designing sets and costumes for a Moscow play. Her revolutionary designs won critical acclaim, and her theatrical career was launched.

In 1921 she joined the Soviet constructionists, artists who put their talents to use for the new communist state. Most abandoned easel painting, even in its most radical forms, as overly bourgeois, and turned instead to design. The general slogan of these 'constructivists' was 'Art into Life', and their goal was 'to unite purely artistic forms with utilitarian intentions'. In their most extreme formulations, the constructivists announced, 'Art is finished! It has no place in the human labour apparatus. Labour, technology, organisation ... that is the ideology of our time.'

For the next several decades Exter produced innovative and influential stage designs for plays, ballets, and experimental films. However, like many radical artists whose work did not fit in with Soviet ideology, Exter eventually left the country, settling permanently in Paris in 1924. There she remained an important influence through her exhibitions, her stage work, and her teaching. Exter continued experimenting and sometimes incorporated modern industrial materials such as celluloid and sheet metal into her futuristic designs.

Just before she immigrated to France, she worked with the Soviet film director Yakov Protazanov (1881-1945) in the production of *Aelita, Queen of Mars.* Protazanov was called "the old man" in Soviet film because he had started his career before the revolution, and he commanded considerable respect. The movie was – for its day – a major production which started in February 1923 and took over a year to complete. There was shot 22,000 meters of film, which resulted in 2,841 of the final movie. The movie opened 30 September 1924 at the Ars Cinema in Moscow, and a special musical score (by Valentin Kruchinin) had been composed to accompany the silent scenes.



The story is based on a novel by Alexei Tolstoi, a distant relative of the famous author Leo Tolstoi. He had actually gone into exile, but had voluntarily returned to the Soviet Union to join the team making the film. Very little of his novel was used for the film, and Tolstoi was deeply disappointed.

The plot was rather simple. The story starts in December 1921 in the chaos of Civil War in the Soviet Union, and the start of the New Economic Policy. An engineer working

among the starving masses of Moscow designs a spacecraft with a friend, who is a solider. Together they go to Mars, and find there a society divided into a ruling class and a working class.The engineer falls madly in love with the Queen of Mars, Aelita. But she is oppressing the workers, and as a good Bolshevik, the soldier starts an uprising among the slave workers of the planet.

At an international exhibition of decorative arts 1925 in Paris, Protazanov was given an award for *Aelita*, at this time Alexandra Exter already had settled there.

Her designs for the movie were remarkable and cubistic. The sketch reproduced shows the costume for one of the oppressed workers. It is angular, making the associations to a machine not far-fetched.[7]

Aelita become an international success and was also exported to the United States. In English it had the sub-title "Revolt of the Robots". The play by Čapek was current at the time *Aeltia* was released, and the theme of *R.U.R.* was similar to that of the film, the oppression of workers by the upper classes. In the sub-title, "robots" retained its original meaning of "machinelike men", or slave workers used without respect for their individual rights as human beings, but rather like tools in an industrial process.

We also realise that my interpretation of the title of Alexandra Exter's little figure in the Art Institute of Chicago was not correct. It was made in 1925, a year or so after the design of the costumes to the slave workers of Mars. It does not render a manlike machine, a "robot" in modern terminology, but rather a machinelike man, a "robot" in the sense of Čapek and *Aelita*. Its association with a machine is a political comment on the exploitation of workers like they were parts in a huge, industrial process.

We therefore still have to find how the word changed its meaning.

6. Fritz Lang and Metropolis: The riddle explained

One of the finest movies ever made is Fritz Lang's *Meteropolis,* it is even indluded in the UNESCO list of the Memory of the World. It was produced in Germany 1925-26 by the Austrian film director Fritz Lang (1890-1976), who escaped to the United States before the Second World War and continued to make memorable movies.

The movie is based on the novel *Metropolis* (1927) written by Lang's wife, Thea von Harbou (1888-1954). The production of the film was itself a major undertaking, new cinematographic techniques were developed, in some of

---

[7] I am gratfuel to the Arts Institute of Chicago to have provided material on Alexandria Exter and her designs for the film.

the scenes, as much as 36,000 extras participated. It was produced by Universum Film AG (Ufa) in Berlin, and nearly brought the company to bankruptcy.

The film is to some extent inspired by *Aelita,* and the story has many parallels both with *Aelita* and *R.U.R.*

The story is set 100 years in the future (2026), in a mighty city like a Gothic version of Manhattan. There are the privileged few and the oppressed workers. The Master of Metropolis is John Masterman. His son, Freder, happens to meet a girl, Maria, in the subterranean city of the workers, where they struggle among the machines, ruthlessly exploited by the privileged. Maria encourages the workers to rise against the tyrants. The Master of Metropolis becomes concerned both with his son's infatuation with Maria, and Maria's radical agitation.

So far in the plot, the parallels to the former versions of the uprising of the workers are rather clear. But a new element is now brought into the story, the evil scientist Rotwang – a figure which still haunts science fiction. Of course he is a genius. And his right hand is replaced by prosthesis and covered in a black glove.[8] Rotwang is asked to make an artificial copy of Maria, which is to take her place in front of the workers and render them harmless, at the same time provide a solution for the lovesick son.

The plan, of course, fails. But in our context, the creation of the artificial Maria, played by a magnificent Birgitte Helm (1906–1996), is important. In the laboratory of Rotwang, the real Maria is placed in an apparatus, and by her side, is placed.a copy of her in metal Using electricity, the life force of the human is transferred to the machine. The laboratory does echo the operating theatre of Dr Frankenstein, where he harnesses the electrical power of lightening to bring his monster to life.

The artificial Maria cannot be mistaken for an android; she is built of metal and circuitry. So in her we encounter a "robot" in the modern meaning of

[8] Stanley Kubrick's *Dr Strangelove* (1964) also wears such a glove over his artificial hand as a tribute to Lang.

of the word. But the word "robot" is not used to describe the artificial Maria, neither in the film nor the novel.

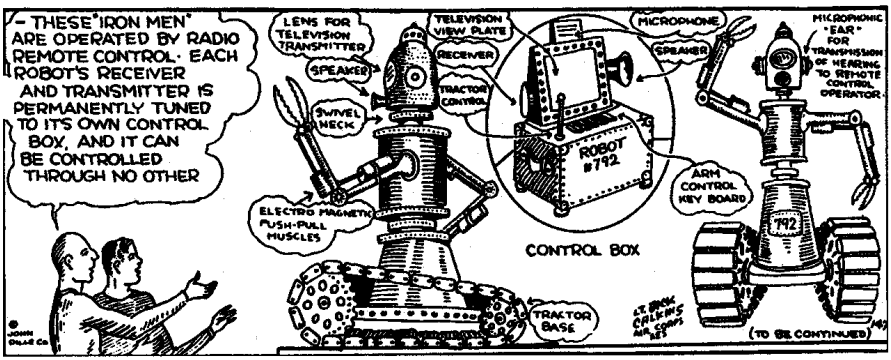
Though *Aelita* was made a couple of years prior to *Metropolis,* they were distributed to the American market about the same time. The themes of the two science fiction movies were rather similar, and both movies were spectacular by the standards of the time – though *Aelita* could not rival *Metropolis* in the force of the allegory told.

In *Aelita,* the subtitle was 'Revolt of the robots', and the workers were dressed in cubistic costumes associating them with mechanical beings. In the other, a humanoid clearly built of metal leads the uprising of the workers.

It seems to me that this is the explanation of how the word "robot" subtly changed its meaning, from "machinelike man" to "manlike machine". In the wake of the popularity of the two movies, the riddle of the robots is explained.

7. Robots entering popular culture: Buck Rogers in the 25th Century

In 1928, the science fiction magazine *Amazing Stories* published the novella 'Armageddon 2418 A.D.' by Philip Francis Nowlan (1888-1940). The story caught the interest of John Dille Company, who contracted the author to develop a comic strip based on the same basic idea. The result was *Buck Rogers in the 25th Century,* one of the first true space operas to be created, and a forerunner for other well-known romances like that of Flash Gordon (and his companion, the scientist Dr Zarkow).



The first episode, 'Meeting the Mongols', is drawn by Dick Calkins and was published in 1929. In this one finds a detailed drawing of something called an 'iron man' – it has video cameras for eyes, speaks through a loudspeaker, the arms end in pliers, and it is moving on rolling belts like a tank. It

is not autonomous, but rather operated at a distance – and would therefore perhaps not earn to be called a 'robot' according to the modern usage of the word. But this is exactly the term used by Nowlan, the iron man bear the brand 'Robot #792'.

This is the earliest example I have found of the word definitely having changed its meaning. *Buck Rogers* became very popular as the first comic strip addressed to an adult audience. The strip ran in US newspapers 1929-1967, the last feature film was made as late as 1979, and a television series run for several seasons, ending in 1981.

The first short-story I have found using the term "robot", is Harl Vincent 'Rex' (*Amazing Stories* 1934), but there were several stories of intelligent or manlike machines around the same time. The robots became a theme in science fiction, the stories typically recalls the original Frankenstein motif, the created intelligent machine turning against its creator.

There are a few anthologies which will give broad samples of the stories of this time: Isaac Asimov, Patricia S Warrick and Martin H Greenberg (eds) Machines that think *(Holt, Rinehart & Winston, New York 1983) and Sam Moskowitz (ed)* The Coming of the Robots *(Collier, New York 1963).*

8. The modern robot: Isaac Asimov and the three laws of robotics

The image of the modern robot was forged by the extraordinary prolific and diverse Isaac Asimov (1920-1993), an American science fiction writer with a Russian background. His first short story on robots was 'Robbie' (*Super Science Stories* 1940). The same year, Asimov brought a proposition for a new story to one of the most influential science fiction editors ever, John W Campbell of *Astounding Stories.*

'My notion was to have a robot refuse to believe he had been created mechanically in a factory, but insist that men were only his servants and that robots were the peak of creation, having been created by some godlike entity. What's more, he would prove his case by reason, and "Reason" was the title of the story.[9]

[9] Isaac Asimov In Memory Yet Green: The Autobiography of Isaac Asimov (Doubleday, New York 1979:281).

The story was published in *Astounding Stories* 1941. In our context, it may be important to emphasise that Asimov in the story, still revolves around the Frankenstein motif, the relation between the creator and the product of the creative process. The robot and its two constructors are in an artificial satellite orbiting the Earth, there being no direct evidence of the human society producing the autonomous robot, which is brought to consciousness for the first time aboard the satellite. It argues with considerable force that the two men cannot have created it:

> *'Look at you. I say this in no spirit of contempt, but look at you! The material you are made of is soft and flabby, lacking endurance and strength, depending for energy of the inefficient oxidation of organic material. Periodically you pass into a coma and the least variation in temperature, air pressure, humidity, or radiation intensity impairs your efficiency, You are* makeshift.
>
> *'I, on the other hand, am a finished product. I absorb electrical energy directly and utilize it with an almost one hundred percent efficiency. I am composed of strong metal, am continuously conscious, and can stand extremes of environment easily. These are facts which, with the self-evident proposition that no being can create another being superior to itself, smashes your silly hypothesis to nothing.'*

The final addition to the modern robot was the three laws of robotics that has made Asimov famous, but which he himself attributes to Campbell from a conversation 23 December 1940:

8.1 The three laws of robotics

1. A robot may not injure a human being, or, through inaction, allow a human being to come to harm.
2. A robot must obey the orders given it by human beings except when such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with First or Second Laws.

On the basis of these laws, Asimov created a series of stories. The short stories are collected in *I, Robot* (1950) and *The Rest of the Robots* (1964). The novels include *Caves of Steel* (1954) and *The Naked Sun* (1957). Towards the end of his career, Asimov started a project of intertwining his robot tales into the original *Foundation* trilogy, and it is difficult to sort out their rela-

tions. Now has also been added the movie *I, Robot* (2004) directed by Alex Proyas (1963-), and based on the characters and plots from the robot stories.

9. Artificial Intelligence, replicants, cyborgs and other family members

It would be futile trying to follow in detail the image of the intelligent machine in fiction after Asimov introduced the modern robot. There are numerous and examples. One will find that in science fiction, robots lived strangely apart from proper computers. When the computers were introduced, the image was of a very large machine, typically a computer that governed society. The miniaturisation and distribution of computers that took place throughout the late 1970s, had not been foreseen in the literature.

A typical image of the intelligent computer is presented in the legendary movie by Stanley Kubrick (1928-1999) *2001: A Space Odyssey* (1968) based on a script by Arthur C Clarke (1917-), a British science fiction author with a crisp, nearly academic and matter-of-fact style. The computer is governing the space vessel journeying to Jupiter, and is called HAL (an obvious pun on IBM). The force of the image of this computer is partly its soft and emotional voice, and the way it develops some sort of paranoia, a mental disorder making it even more human. It may be maintained that in this respect, the Frankenstein motif again emerges – at least, the dialogue between man and machine is part of a discussion of what essentially makes a human being different from an intelligent machine.

This becomes one of the major themes in the work of the American science fiction author Philip K Dick (1928-1982). In his many books and stories, he has really only one major question, 'What is reality?' His own tongue-in-cheek answer is, 'Reality is what refuses to go away when I stop believing in it.' In all his books he finds a new way of discussing the relation between reality and images of reality.

An important version of his basic question is how to see the difference between a human and an imitation of a human. The novel in which this question perhaps is most clearly in focus, is *Do Androids Dream of Electric Sheep?* (1968). "Androids" are, of course, the name given to an artificial being not constructed from metal, but rather from organic material. In the novel, androids are prohibited from visiting Earth, and have a very limited life-span. Rouge androids frequently trespass, and a corps of law enforcement officers hunts them down, administers tests to make sure they

have caught an android and not a human being, and then 'retire' them. The protagonist of the novel is such an officer, and he becomes deeply troubled when he finds it difficult to identify androids, when he also falls in love with one of them and, finally, starts to believe he himself may be an android.

The novel has become even better known in the movie version, *Blade Runner* (1982), directed by Ridly Scott with Harrison Ford in the role as the protagonist. In the film, the androids are called "replicants", emphasising the central issue of similarity between the hunter and the hunted.

I a way, this closes the ring. We started out with the robots of Čapek, being produced from organic material in chemical vats, and ends up with the replicants, sophisticated and smart look-alikes to humans. But there is still one more step to go – the fusion or union between man and machine, the cybernetic organism, the cyborg.

In the 1980s, there appeared a strain of science fiction usually called "cyberpunk". There are several prominent authors that could be counted as belonging to this school, but the exponent is William Gibson (1948-), who in his first and vibrant novel *Neuromancer* (1984) coins the word "cyberspace", which has been absorbed by everyday language as a reference to the virtual reality of computerised networks and machines. In the work of Gibson and the other cyberpunkers, the computer is directly interfaced with the neural network of man. An extra memory chip may be slotted into a socket behind the ear for easy access to a foreign language; a readout from you personal agenda is available in your field of vision, including a face recognition module to prompt you for the name of a person you have met in a cocktail party, outlining his personal information as he told you at that occasion – supplemented with what is available on the Net. And for a high, the pleasure centre of the brain is directly stimulated by an inserted probe …

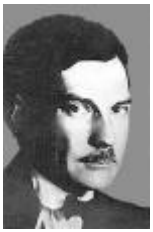
In this emerging fiction, the distinction which has followed us through this essay – between "machinelike man" and "manlike machine" – is absorbed in a new synthesis, which may be an apt symbol for the post-industrial society. Frankenstein's monster was born from the emerging understanding of the power inherent in natural sciences. The robots were an allegory to the social and political forces in the industrial society. The cyborg may be the symbol making explicit the new and ethical challenges when biotechnology, nanotechnology and information technology converges into new possibilities both for the individual and society.

10. Postscript: The PIN and Zamyatin

In this essay, the robot has been considered as a powerful literary symbol, emphasising the way humans may be used without respecting their individual dignity, as machines in an industrial production system. It has occurred to me that there is one other such symbol, this is the number – it is often used as slogans, 'Individuals are reduced to numbers in the machinery of bureaucracy,' or similar statements.

The reason for the number having this symbolic effect has not been quite clear to me. One might think it was related to the introduction of early computerised systems, where storage capacity was scarce, and where numbers were somewhat more easily handled than letters. Some countries have introduced personal identification numbers, a unique number used typically in the communication with government systems to avoid mistakes of identity. Obviously, numbers are also used for similar purposes by countries not having a unique PIN, like the social security number in the United States, or the tax administrative number in Canada.

But clearly the symbolic value assigned to numbers predates government computer systems. Perhaps some of the negative associations are related to the use of numbers tattooed onto the skin of prisoners in German concentration camps during the Second World War. But this only must have augmented a quality of 'the reduction to a number' already present. Perhaps also this has a literary explanation – at least there is a powerful Utopian novel from the time of the Soviet revolution which, as far as I know, for the first time introduces numbers as a symbol of the lack of respect for human individuality.



Yevgeny Ivanovich Zamyatin (1884-1937) was a powerful literary figure in the early Soviet state. He welcomed the revolution, he criticised its repression of freedom. He was close to the leaders of the revolution, but was arrested several times, and become considered a heretic, constantly attacked in the late 1920s by Communist Party-line critics. He had to give up the leadership of the All-Russian Writers' Union. His works were banned, removed from libraries, and he was unable to publish. After writing a letter to Stalin, Zamyatin was allowed to go with his wife into exile in 1931. He settled in Paris in 1932, where he died in poverty.

He completed his only novel, *We,* in 1921. Extracts from the original text were published in an émigré journal in Prague in 1927. In Russia *We* circulated in manuscript, and was finally published in Paris.

Zamyatin's *We* (original title *My,* 1921) takes place in the One State, where all buildings, tools and machines are made of glass. People are called 'numbers' and all live, work and act precisely in unison, to the point that they chew their food together. Their actions are dictated by the Table of Hours, a

clock system which synchronises precisely what everyone is to do and when. The people are ruled by the Benefactor and policed by the Guardians. The protagonist is D-503, a mathematician and builder of the Integral, a gigantic glass space-ship which is being constructed to go to other planets and spread the joy of the One State – here one may see the a parallel to *Aelita*.

One will recognise the theme of the novel as common to that of the two most influential utopian novels of the last century, *Brave New World* (1932) by Aldous Huxley (1894-1963) and *1984* (1949) by George Orwell (1903-1950), as well as closely related to that of the revolt of the robots in *R.U.R, Aelita* and *Metropolis.* It indicates that the web of literary symbols and allegories are much more complex than we have been allowed to glimpse through the small aperture opened by Alexandra Exter's cardboard figure in the Art Institute of Chicago. We will not pursue these tantalising threads to find new and intertwining patterns. But they remain reminders not only of the richness of the literary imagination, but also of the importance to our understanding of ourselves, and our relation to the society contained in these symbols and allegories.

I am pleased and satisfied to have solved, at least to my own satisfaction, the riddle of the word "robot".

2 KAN FORBRUKERKJØPSLOVENS REGLER ANVENDES FOR DIGITALE YTELSER?[1]

Av Olav Torvund

Finnes det et marked?

Markedet for nedlastingstjenester er i dag ikke særlig stort. Den største omsetningen gjelder noe så unyttig som ringetoner til mobiltelefoner. I oktober 2003 opplyste TONO at det ble lastet ned ca 150.000 ringetoner pr måned, og det er ingen grunn til å tro at dette har avtatt.

For musikk ser vi at det stadig kommer til nye tjenester for lovlig nedlasting av musikk. I Norge er foreløpig MusikkOnline[2], som tilbys av Phonofile, en eneste innenlands tjenesten. Internasjonalt er Apples tjeneste *iTunes* den som til nå har hatt størst suksess. Apple har gjennom denne tjenesten vist at det er et marked for slike tjenester.

Dataprogrammer er antageligvis den produktgruppen hvor denne leveringsformen så langt er mest vanlig. Men her er det vanskelig å få noen oversikt over markedet. Dette er et internasjonalt marked. Det er grunn til å tro at en stor del av leveringen til norske kunder skjer fra utlandet. Samtidig opplyser norske leverandører at de fleste av deres kunder er utenfor Norge. Som eksempel har *Opera Software*, som omsetter for 15-18 mill pr år i dette segmentet, bare ca 1% av sine kunder i Norge.

Det er imidlertid grunn til å tro at dette markedet vil bli betydelig større i en ikke alt for fjern fremtid. Materiale som vi i dag kjøper på CD eller på papir, vil i stigende grad leveres på denne måten. Men vel så spennende er kanskje mulighetene for å få tilgang til materiale som i dag *ikke* er tilgjengelig for folk flest. I *Jazzbasen*[3] og *Norsk folkemusikkarkiv*[4] finnes f.eks. store musikksamlinger som vil kunne gjøres tilgjengelig. Og de som ikke er spesielt

---

1 Artikkelen er basert på en utredning om Forbrukerkjøpslovens anvendelse ved levering av digitale ytelser utført for Justisdepartementet. Utredningen finnes på http://www.odin.no/jd/norsk/dok/andre_dok/rapporter/012041-220006/dok-bn.html

2 www.musikkonline.no

3 http://www.jazzbasen.no/

4 http://www.hf.uio.no/imt/om_imt/nfs/saml.html

interessert i smal musikk ville ganske sikkert kunne finne mye interessant i NRKs arkiver,[5] om materalet i disse hadde vært tilgjengelig for nedlasting.

Distribusjonsmodeller

Mye materiale er fritt tilgjengelig. Men det er lite aktuelt å gjøre kjøpsrettslige sanksjoner gjeldende i forhold til materiale man har kunnet laste ned gratis. Så jeg vil her konsentrere meg om modeller for omsetning.

Leverandørenes utfordring er enkel levering, samtidig som man beholder kontrollen med spredningen av det som er levert. Løsningen på dette er stort sett at man leverer filene i kryptert form. Bare den som har riktig nøkkel vil kunne spille av filene. I dag kan man f.eks. finne begrensninger som gjør at de filene bare kan spilles av (fremføres) på bestemte utstyrsenheter. Så lenge dette er en PC man har stående på sitt arbeidsrom, er ikke dette en særlig attraktiv løsning. Det er ikke der man først og fremst ønsker å høre musikk eller se på film. Man ser imidlertid at det etter hvert kommer mer fleksible løsninger, som i noen grad tillater brenning av CD m.m.

Selv har jeg tro på at smartkort vil bli et viktig hjelpemiddel i dette markedet. De aller fleste av oss bruker i dag smartkort, uten at vi helt tenker over det: I våre GSM mobiltelefoner sitter det et SIM-kort, med all nødvendig informasjon om vårt abonnement. Når vi faller for fristelsen til å kjøpe en ny mobiltelefon, trenger vi ikke gjøre annet enn å flytte det gamle SIM-kortet over i den nye telefonen. Det er heller ikke vanskelig å få utstedt et nytt kort, om det skulle være nødvendig. På en tilsvarende måte bør det være mulig å administrere tilgangen til nedlastede filer. Med et "SIM-kort" i avspillingsutstyret kan man spille av alle filene, og man kan flytte det om man kjøper nytt utstyr. Det bør heller ikke være vanskelig å ha flere kort for samme bruker, slik at man kan spille av filene på ulike enheter. Men foreløpig er dette ikke tilgjengelig – i alle fall ikke som jeg kjenner til.

Dagens regler

Sett fra et praktisk synspunkt er spørsmålet om nedlasting eller levering på CD bare et spørsmål om valg av leveringsmåter. Hvis vi har tilstrekkelig båndbredde og filene ikke er for store, er nedlasting mest praktisk. Fordelen er at vi får ytelsen med en gang, uten å måtte vente på at en pakke skal leveres. For forbrukere skal man heller ikke se bort fra at nedlasting kan være mer fristende fordi de

[5] http://www.nrk.no/informasjon/om_nrk/1774258.html

signalene som overføres ikke går innom tollmyndighetene på veien fra en utenlandsk leverandør til forbruker. Men å laste ned flere hundre megabyte uten en ganske rask bredbåndsforbindelse, er lite hensiktsmessig.

Rettslig sett er imidlertid transaksjonene svært forskjellig. Hvis vi får levert et stykke plastikk i form av en CD-plate, så *kjøper* vi CD-platen. Man kan argumentere for at det er de dataene som platen er bærer av og ikke plastplate i seg selv som er interessant og gir den verdi. Men det samme kan man si om musikk-CDer, bøker, osv. Vi kjøper ikke bøker for å skaffe oss papir og trykksverte. Likevel er det ingen tvil om at dette er kjøp.

Velger vi å laste ned filene, skjer det ingen levering av en fysisk gjenstand. Denne ytelsen består av to elementer: Vi får for det første en *lisens* som gir oss rett til å fremstille et eller flere eksemplarer av filen. For det annet yter leverandøren en tjeneste som gjør det mulig å laste ned filen.. Ingen av disse elementene vil være kjøp.

Opphavsrettslig er de to transaksjonstypene ganske forskjellige. Hvis jeg kjøper en CD, kjøper jeg et *eksemplar* av verket. Dette eksemplaret kan jeg i medhold av *åvl § 19* låne bort, og jeg kan ikke minst selge det videre. Hvis jeg i stedet velger å laste ned filene, ender jeg også med et eksemplar. Men dette eksemplaret har jeg ikke kjøpt, jeg har produsert det i henhold til den lisensavtalen som jeg har inngått. Siden jeg ikke har kjøpt eksemplaret, har jeg ingen rett til videresalg m.m., ut over den rett som lisensavtalen eventuelt måtte gi. Og i praksis gir ikke den noen rett til å overdra et slikt eksemplar.

Heller ikke selve lisensen kan overdras med mindre man har samtykke. Dette følger av *åvl § 39b annet ledd*, som sier at en ervervet opphavsrett ikke kan overdras videre uten samtykke. Lisensen er en opphavsrettslig beføyelse. Selv om den ikke er særlig vidtrekkende, så omfattes den like fullt av bestemmelsen.

Uten at det er tilsiktet, får den forbruker som velger nedlasting en svakere stilling enn den som får filene levert på et fysisk lagringsmedium. Det er grunn til å sette også denne type forbrukerspørsmål på dagsorden: Hva slags (minimums)rettigheter bør en forbruker få når han laster ned en fil mot betaling.

Det er imidlertid ikke disse spørsmålene som jeg skal diskutere i det følgende. Jeg skal holde meg til det langt mindre vidtrekkende spørsmålet om forbrukeren også ved levering av digitale ytelser bør nyte godt av det samme forbrukervernet som ved kjøp av fysiske gjenstander. Forbrukerkjøpsloven er preseptorisk innenfor sitt område. Om en avtale gir forbrukeren dårligere rett enn det han etter loven skal ha, så går loven foran. Men faller vi utenfor lovens området, faller transaksjonen utenfor preseptorisk lov. Og da vil det kunne avtales vilkår som er langt dårligere for forbrukeren. Riktignok vil *avt § 36* sette en grense for hva slags avtaler som kan inngås. Men det er ganske langt fra forbrukerkjøpslovens regler til det som kan settes til side som urimelig i medhold av *avt § 36*.

Bør digitale ytelser omfattes av forbrukerkjøpsloven?

Da jeg gikk i gang med vurderingen av om forbrukerkjøpsloven kunne tilpasses digitale ytelser, hadde jeg en forventning om at dette kunne bli vanskelig. Men det skulle vise seg at forbrukerkjøpslovens regler enkelt lar seg tilpasse også denne type ytelser.

Velger man å la forbrukerkjøpsloven omfatte digitale ytelser, må det nødvendigvis foretas en justering av bestemmelsen om lovens anvendelsesområde i § 2. Men dette vi være en liten justering.

Det er heller ingen grunn til å fravike prinsippet om at man ikke kan avtale at annet lands rett skal gjelde. Rekkevidden av en slik bestemmelse vil i praksis kunne være begrenset når levering skjer fra utlandet. Men disse spørsmålene går jeg ikke nærmere inn på.

Siden leveringsmåten vil være vesenforskjellig, skulle man tro at reglene om levering vanskelig kan overføres. Men det grunnleggende prinsippet for hentekjøp, om at selger skal holde ytelsen tilgjengelig for kjøper, lar seg enkelt overføre. Ytelsen må holdes tilgjengelig på en annen måte, men det endrer ikke utgangspunktet. Man kan også anvende prinsippet om at levering har skjedd når tingen overtas, som i en digital verden vil si at man har fått overført filen på en slik måte at man kan nyttiggjøre seg denne. I dette siste ligger at man også må ha fått overført eventuelle lisensnøkler m.m. som måtte være nødvendige for å kunne nyttiggjøre seg filene.

De øvrige bestemmelser om levering er så spesifikt knyttet til fysisk levering at de i praksis ikke vil komme til anvendelse for digitale ytelser. Men nettopp derfor kan de også videreføres uten noen tilpasninger.

Spørsmålet om risiko er direkte knyttet til den fysiske gjenstanden. Det er lett å se problemstillingene som dukker opp hvis den ytelse som skal leveres ødelegges i brann eller på annen måte blir ødelagt av en tilfeldig hendelse. Men rettigheter blir ikke ødelagt. Om mitt eksemplar skulle bli ødelagt, så mister jeg ikke automatisk mine opphavsrettslige beføyelser. Dersom jeg har opptrådt etter læreboken, vil jeg kunne gjenskape det tapte eksemplaret fra en sikkerhetskopi og har lisensen i behold.

Det eksemplar man har fremstilt i henhold til lisensen, kan imidlertid bli ødelagt på mange måter. Og de fleste av oss er nok ikke så påpasselige med sikkerhetskopier som vi kanskje burde være. Langt mindre dramatiske hendelser enn en brann, f.eks. diskkræsj, vil kunne gjøre eksemplaret ubrukelig. Det er liten tvil om at risikoen i kjøpsrettslig forstand på dette tidspunkt vil ha gått over til kunden.

Men samtidig er det slik at leverandøren ikke behøver å produsere og levere et nytt eksemplar for at brukeren igjen skal få tilgang til det. Leverandøren trenger bare å gi kunden tilgang til nedlastingstjenesten på nytt, slik at kunden kan fremstille et nytt eksemplar. Når leverandørens kostnader vil

være små, er det ingen grunn til ikke å gi kunden en rett til å laste ned de nødvendige filene på nytt. I mitt forslag til Justisdepartementet har jeg ikke gått inn for at leverandøren skal ha noen plikt til å holde gamler versjoner tilgjengelig. Men hvis ny nedlasting kan skje uten vesentlig kostnad eller ulempe, bør forbrukeren ha en slik rett.

Når det gjelder kravet til den leverte ytelse, er det ingen grunn til å gi kunden ulike rettigheter avhengig av leveringsmåten. Riktignok vil mediefeil ikke ha den samme praktiske betydning ved nedlasting som ved levering av ytelsen på fysiske medier, men det skaper ingen særlige rettslige problemer. Men er det innholdsmessige feil i den leverte ytelse, f.eks. slik at et levert dataprogram ikke fungerer som forutsatt, så er det ingen grunn til å forskjellsbehandle kundene bare fordi disse har valgt ulike leveringsmåte.

Dersom det skulle bli aktuelt å heve avtalen som følge av mangler, er utgangspunktet at hver av partene skal levere tilbake den ytelse de har mottatt. Å levere tilbake en lisens er ikke særlig praktisk, men den vil falle bort dersom avtalen heves. Noe eksemplar har kunden ikke fått fra leverandøren, slik at det heller ikke blir noe som skal leveres tilbake. Men faller retten til eksemplaret bort, må kunden være forpliktet til å tilintetgjøre det. I praksis må de nedlastede filene slettes. Leverandøren kan være bekymret over at han ikke får en fullgod kontroll med at filene virkelig blir slettet. Men er den leverte ytelse beheftet med så alvorlige mangler at de gir kunden rett til å heve, så er det ikke særlig sannsynlig at ytelsen har noen verdi, verken for kunden eller andre som dette kunne ha vært overført til. Det er heller ingen grunn til at en slik usikkerhet skal svekke kundens posisjon i denne situasjonen.

Konklusjonen i utredningen er at det kun er nødvendig å gjøre fire mindre endringer i forbrukerkjøpsloven for at denne også skal kunne anvendes på digitale ytelser. I utredningens pkt. 10.9 oppsummeres disse slik:

§ 2 om lovens anvendelsesområde må endres.

Prinsippet i *§ 5* vil kunne anvendes uendret. Men i og med at bestemmelsen så klart er formulert med sikte på levering av fysiske gjenstander, bør bestemmelsen få et tillegg som presiserer plikten til å sørge for at filen er tilgjengelig for nedlasting.

I kapittel 3 bør det tas inn en rett for forbrukeren til å kunne laste ned en fil på nytt, eventuelt å få levert på nytt en kode som er nødvendig for å kunne benytte filen, og dette kan skje uten vesentlig kostnad eller ulempe for selger, også etter at risikoen har gått over på kunden.

Plikten til å tilintetgjøre eller gjøre ubrukelig fremstilte eksemplarer ved heving, bør tas inn i *§ 49*.

3 MAKING ACCESS RIGHTS OPERATIVE

By Professor Dag Wiese Schartum,
Section for Information Technology and Administrative Systems, University of Oslo

1. Introduction

Access to government-held information ("access") is, to a large extent, about the right and opportunity to acquire knowledge concerning government actions and relations in order to evaluate and, potentially, take informed political or legal action. I define information as "government-held" if it is either produced or received by a government agency. In this article, access to government-held information is discussed both as a formal right and a question of citizens' ability to exercise their rights. This article is based on the Norwegian experience, but I have refrained from discussing detailed, substantive legal questions. Instead, I have emphasised the significance of statutory structures and types of measures that are contained in "access legislation" in both Norway and many other countries. One of the important perspectives that I have attempted to establish is that statutory instruments – however much they may have been improved – are in themselves limited. Therefore we need to ask: how do we move forwards? How might we make access rights operative? My contribution to this discussion is, first and foremost, to propose perspectives, procedures and categorisations.

For a long time, access to government-held information has been recognised as an important element of democracy, proven, for example, by the adoption of freedom of information legislation.[1] Such rights are crucial to our ability to control and criticise government, and as a basis for proposing alternative policies. Furthermore, access rights are important in a society under the rule of law, as a measure of individuals' ability to pursue their economic, social and ideological interests. Since government holds a central position in our societies, access rights not only effect our relations to government. Where government plays the role of intermediary and decision-maker, access rights may even affect our relations to private parties.

---

[1] In Norway, "offentlighetsloven", or Act Regarding Access to Government-held Information, was enacted in 1970.

The access examples that I highlight are rational, in the sense that accessing information is assumed to occur for concrete and obvious reasons. This approach overlooks important aspects. For instance, access rights may be regarded as having a considerable educational quality, which may be of significance for the dissemination of relevant knowledge among citizens, and thus to the extent and character of their democratic participation. Moreover, access rights may have an impact on the opportunity for self-realisation. The granting or denial of access to information, and thus the development of knowledge, may influence which layer of society a person has access to, and, thereby, the type of social actor he or she is able to develop into.

This article voices a "democratic-political" rather than a "democratic-commercial" approach, meaning that emphasis is placed on access rights as a tool for political participation rather than as a means to do business in the information market place. One obvious consequence is that possible synergies between public administration and private information market place actors are not given special attention. On the other hand, it would be a misconception to assume that a "democratic-commercial" approach conflicts with a "democratic-political" viewpoint. On the contrary, access to government-held information by business actors can be regarded as one of the prerequisites for effective access rights for citizens and their participation in the political and legal systems. It is unlikely that many governments will develop adequate tools for the effective scrutiny of government policy by citizens. Thus, private business initiatives can, and should, contribute positively to the development of applications that facilitate the effective exercise of access rights.

Are there grounds for believing that questions regarding access to government-held information are more important in 2004 than previously? I will highlight a number of elements that may indicate such a growing importance, though more linked to our phase in history than to a particular year. We live in a time of great political and administrative change, in particular with regard to changes in decision-making processes and reorganisation within and between government agencies. Internationalisation, European integration, modernisation and new public management are key concepts that describe elements in this development. Such changes are fundamental and challenge our democracies by their extensiveness, intensity and speed. As a consequence, the volume and complexity of accessible information is likely to become greater than ever before. At the same time, information and communication technology (ICT) may facilitate more effective processing of information, included processing to improve access. On the other hand, we remain, by and large, equipped with access legislation from a time when national and traditional government existed in a comparatively primitive tech-

nological context. This somewhat paradoxical situation calls for analysis and proposals for how to move forwards.

2. Documenting government conduct

The very existence of comprehensible information is an obvious prerequisite for effective access rights. Thus, before analysing these rights, I will briefly discuss the extent to which government administration generates information that citizens may have access to. Obviously, comprehensive rights are of limited value if there is little to access!

My starting point is a simple distinction between "transient" and documented information. By transient information I refer to information that leaves no traces, thus preventing others than those present from making a subsequent evaluation of the content. Examples of transient information include information derived from the spoken word and that contained in physical action. Provided that a recording device is used, such transient information can be documented, i.e. a representation of the information generated, making the data available for subsequent access. Access rights first and foremost relate to accessing documents,[2] but can also comprise access to transient information, such as meetings by decision-making bodies. The value of access to transient information is limited because it is conditional on personal presence and physical access. Thus, potential change in the balance between these two main categories of information is essential for the future of access rights.

Much of the traditional communication occurring within government organisations (as in most organisations) has been of the transient type. Although bureaucracies are famous for generating documents, a large proportion of communication consists of conversations (telephone, meetings, in corridors etc.). Although the exercise of government power is typically not associated with, for example, the informal exchange of views during lunch breaks, decisions may in fact be based on transient communication over a nice cup of tea. To the extent that citizens should have the opportunity to access information contained in such transient exchanges, at least three strategies may be adopted:

- Government may *document selected and significant elements* of transient information. For instance, requiring that decisions are documented in

[2] "Document" is widely defined, covering paper documents, images, video and sound recordings, drawings etc, see AGI section 3.

writing and grounds given, or that officials be obliged to note case-relevant contents of conversations with parties to the case.[3]

- Secondly, transient information may be *recorded* so that a representation of the real-life event is produced and made accessible to citizens. An example of this is images and/or sound from meetings.
- Thirdly, government may create *formal situations* were the spoken word is recognised as publicly accessible information – typically meetings of government bodies to which the public has access.

ICT may obviously be used to record transient information and thus ensure that more information is available for citizens. This can be the case with regard to meetings of political bodies to which the public have access. One clear advantage is that such recordings constitute a document that can be placed in context with other documents relating to the same case. Even in individual cases, telephone calls between officials in charge and between officials and parties to cases can be recorded. Such recordings may, for instance, be defined as case documents, filed and made available to the party by means of an internet-based routine.

Extensive use of email may be deemed to indicate that previously transient information is increasingly communicated in a manner that produces documented information. If so, such a development may be regarded as progress in increasing the accessibility of information. However, Norwegian law does not define email logs as registers to which everybody has guaranteed access, and not every email is automatically classed as a case document. Only those email messages that are defined by the official in question as government case documents are recorded in the correspondence list and made accessible in accordance with the Act Regarding Access to Government-held Information. Thus, the enormous volume of emails logged does not necessarily imply a notable increase in the number of publicly accessible documents. However, government agencies are at liberty to disclose any email message that is relevant to government activity, with the exception of emails covered by secrecy provisions. In reality therefore, access is not dependent on the rights of citizens but on the accommodating attitude of government, a state of affairs that strongly limits the real value of such access.

The other side of the coin when discussing email and access rights is a possible reduction in the amount of accessible documentation. In the same way that email may replace telephone calls, email may also reduce the use of traditional posted letters. Both types of communication generate documents and are therefore, in principle, accessible. However, while correspondence

[3] cf. Public Administration Act (hereafter: PAA), section 11 d.

using official letterhead is obliged to be filed, the filing of emails is dependent on a conscious evaluation of the information contained in the message. Thus, if email is chosen in favour of an official letter, it is less certain that the document will be regarded as a case document and to be filed in the correspondence list.

The period of time during which documents exist is, of course, of crucial importance to the right to access government-held information. In Norway, the Archives Act[4] regulates which documents are handed over to the National Archive of Norway (Arkivverket). In addition, the obligation to keep case records etc. may follow from other special laws regulating narrower fields. On the other hand, legislation may lead to the deletion of documents or items of information contained in documents. This is particularly the case regarding personal data that is deleted once the purpose of its processing does not warrant further storage.[5] However, such personal information may, in principle, be retained if the information is to be transferred to the national archive authorities.

I lack the basis upon which to decide whether or not ICT leads to changes in the balance between transient and documented information. Here, my main point is that technology can be employed to generate documents in situations were it has traditionally been awkward, even impossible, to produce documents which may subsequently become objects for access rights. In particular, formal situations, such as meetings where government powers are exercised, may in many instances be documented by automatic procedures. This is also the case for telephone conversations and the exchange of emails with parties to cases. The basis for access to information may be broader than before, but thus far there are no signs of such a development in Norway.

3. Fragmented access regulation

Access rights are rooted in our societies. I will not discuss how we should describe this "root", but have instead chosen the simple approach of referring to the following three legal-political principles, which describe fundamental qualities of government:

- Freedom of information
- Rule of law
- Data protection

---

4 Act 1992-12-04-126.

5 cf. PDA, section 28, first subsection.

I could have chosen a number of other principles and freedoms. "Free competition" would have been an alternative if economic aspects had been of special importance; and "equality" would have been a candidate had social rights been the topic of discussion. I have assumed that all such principles and/or their fulfilment may be said to contain or presuppose access to information. Thus, I could have described the significance of access rights much more extensively than that which follows from the three principles chosen here.

Typically, each of the three selected principles assures the protection of certain rights or particular status for citizens. In Norway (as in many other countries), legislation has been enacted to establish minimum standards governing the legal position of citizens. In the Norwegian context, the following laws are the main guarantors for the three principles:

- Freedom of Information – Act Regarding Access to Government-held Information (of 1970), mentioned before[6]
- Rule of law – the Public Administrative Act (of 1967), hereafter PAA[7]
- Data protection – the Personal Data Act (of 2000), hereafter PDA[8]

In this section, I will discuss the major regulatory designs within which legislators have granted people rights to access government-held information. Contemporary Norwegian information access legislation is, to a large extent, organised with the aim of supporting citizens in particular situations and/or helping them pursue specific goals.

Principle	Freedom of information	Rule of Law	Data Protection
Status	↓ As "citizen"	↓ As "party" to a case	↓ As "data subject"

Table 1

Each piece of legislation corresponds to at least one of the three principles referred to above. Access rights provided, for instance, by the PAA, are based on the assumption that citizens may wish to access their case dossiers in order to pursue their legal interests in cases to which they are party. Similarly, the AGI is based on the assumption that people may wish to fulfil their role as

6 Act 1970-06-19-69, sometimes also translated as "the Freedom of Information Act".
7 Act 1967-02-10.
8 Act 2000-04-14-31.

members of a democratic society by monitoring, or even trying to influence, government. Their motivation may not only be their role as citizens, but also a desire to act to their own personal advantage. Access rights pursuant to the PDA are seen as a way of safeguarding an individuals' rights regarding data protection. Such protection not only regulates access to our own registered personal information. General access rights pursuant to the PDA permit any citizen to seek information regarding the extent and nature of the processing of personal data in society. Moreover, the rights enshrined in the PDA supplement those enshrined in the PAA, because case-relevant personal data may exist outside the case dossiers.

Together, the three laws referred to above give access rights to a large proportion of the population. The AGI and the PDA give access rights to everybody, i.e., in principal, limited only by individuals' curiosity and willingness to take action. The access rights enshrined in the PAA and the individual's rights enshrined in the PDA presuppose that people have a certain formal status. However, the situation of being registered or a party to a case is one that applies to many people. Thus, together, these three sets of access rights are very comprehensive. In addition, access may be requested on the basis of special regulations, i.e. within fields of government where the legislators were of the opinion that special needs existed, either to expand or restrict the access provided by general rights.[9]

Each of the acts mentioned above define a limited set of access rights that have been regarded as sufficient to satisfy the needs of the various assumed purposes and situations. Each access right has, to a large extent, been developed with little direct co-ordination with existing rights, implying that each right exists as an "island" of good intentions. Is it both feasible and desirable to establish a "mainland" of access rights, i.e. a co-ordinated body of access provisions that cover access requirements for a variety of situations and purposes?

The question above may not have one simple answer as it contains several problems and opportunities. Simply merging existing general access legislation into one "Information Access Act" is possible, but would obviously leave great gaps in the other laws were access provisions to be moved into a new act. This is particularly the case with the provisions concerning access rights in the PAA and PDA. Access rights in these laws constitute integral elements of other important guarantees for citizens. Access provisions must therefore be placed close to the provisions with which they interact. It is, for instance, crucial that access rights are placed in the context of the provisions defining information quality standards. A rearrangement resulting in the grouping together of various access provisions under the same statutory roof

[9] Special access rights exist, for example within the health and police sectors.

would weaken the laws they originated from. The benefits that might be gained by collecting access right provisions in one novel piece of legislation may, in other words, be lost because such a regulatory design would not satisfy the need for a fruitful legal context.

A second possibility is to insert a standard body of access provisions into every major act where questions of transparency and freedom of information are regarded as important issues. However, the complexity and volume that would be created by such a strategy makes such a "multiplication strategy" highly problematic.

In our statutory tradition, acts should contain legal norms and contribute to answering normative substantive questions. Thus, simply informing citizens by means of Parliamentary acts, i.e. repeating and/or clarifying norms which form part of other legislation, rarely occurs.[10] In one period following the Second World War, many acts were enacted as "framework legislation", implying that most of the concrete legal norms were delegated and formulated in regulations adopted by the government or a ministry. One way to regard framework legislation is to consider it as norms that i) define limits to the delegated statutory power, and ii) confirm the existence of one or more regulations issued pursuant to the act.

One possibility regarding access regulations is to establish a "hub act", meaning a law that i) defines common provisions regarding access rights (for instance supplementary rules and rules aimed at solving conflicts of interpretation), and ii) contains a meta level description of existing access regulations. Such a description of access regulation may, for instance, consist of rights enjoyed by everyone, and in addition contain an overview of other classes of rights within fields of special interest, for instance the business, health and police sectors. Hub legislation might even contain overviews of access rights pertaining to specific situations, for instance, the access rights that apply if a citizen has a disagreement with a government agency or if an individual buys or sells an estate or shares.

The preceding example concerning shares and estates may illustrate another important benefit were an access law hub to be adopted. Today, we are discussing the proportion of the indistinct zone between government and private sector that is to be covered by the Norwegian AGI.[11] On the other hand, we currently have scattered pieces of legislation that provide the right of direct access to information held in private businesses, and legislation that compels private actors to report information to government, where it may

---

[10] A fairly recent example is section 11 litra a of the PDA, where the reader is reminded of the various steps required to secure compliance with basic requirements for processing personal data, and without any additional effect.

[11] See NOU 2003: 30 Ny offentlighetslov (concerning amendments to the AGI).

subsequently be accessed by anyone. A general access law containing provisions that were independent of the traditional division between private and public sectors would be an obvious gain to many.

The fact that many of the benefits that could be gained through hub legislation might just as well be gained from simple information initiatives is an obvious reason for rejecting the hub legislation option. There is certainly no reason to make things more difficult than necessary, and adopting a new law is just asking for inconvenience and inflexibility. If information related initiatives could have the same effect as hub legislation, then they are probably to be preferred.

The PDA introduced a general obligation for controllers to provide guidance regarding statutory access rights to data subjects.[12] This obligation applies regardless of the nature of inquiry from the data subject, and thus represents an independent obligation to consider the *total* needs and opportunity connected to accessing information. Obviously, this is an ill-placed provision, as it goes far beyond the access rights defined in the PDA. A hub law, as suggested above, may obviously constitute a better systematic placing. Moreover, such an act could contain several provisions that would tie the other access laws together as a bundle of laws. In particular, such a novel piece of legislation could establish common procedures regarding various ways of distributing and obtaining information, see section 4 (below). For instance, a common set of provisions could be established regarding the publication of information and processing access requests from citizens. If I, for example, were interested in accessing information in a tax case, both the tax office and Public Registrar would be relevant addressees. Common procedural rules, laid down in hub legislation, could guarantee that a single access request would suffice to communicate with both addressees and ensure that all possible types of access rights were considered, i.e. regardless of the specific legal basis.

4. Categories of access rights

Which categories of access rights do the PAA, PDA, AGI and other legislation contain? What follows is an attempt to identify and present the various categories of such rights, based on an empirical study of Norwegian legislation. I have assumed that this legislation is better than average – at least in a formal sense – i.e. that Norwegian access legislation is rather "rich", in the sense that it contains many aspects and elements of access legislation that are adequate when a general description is to be deduced. This is not to say that the

[12] See section 6, subsection 2.

legislative basis is in anyway complete, nor do I claim that my construction is complete and fully relevant in relation to any legal system. However, the point here is not the details, but illustrating how aspects and elements of access rights might be grouped within one framework. That said, within the universe of Norwegian access rights, I have made no other obvious simplifications than those described here.

Access on request by the citizen is one of the key enablers for the creation of information openness in the legislation referred to above. In addition, a variety of other laws support access rights by means of a large number of other techniques, which I will identify and describe here. The aim is to make the contents of the legislators' "toolbox" evident in cases where the objective is to establish access rights. I have chosen to divide the techniques into two groups, according to who is required to take action:

a) the duty of government agencies to disseminate information, and
b) the rights of individuals to obtain information.

a) The duty of government agencies to distribute information

In principle, *a duty to publish* represents the widest duty to provide access to information. However, this may be limited to publications with very small circulations, and thus have little tangible effect as a means of informing the general public. In Norway, the duty to publish has, first and foremost, been used in connection with statutory instruments, for instance by establishing a duty to publish every new act of Parliament and regulations pursuant to acts.[13] In 2004, the law was amended, establishing a duty to publish particular statutory instruments and make them available, free of charge and generally available, in an electronic format (in practise on the Internet).[14]

A *duty to make information available* is similar to the duty to publish, but with fewer requirements for proactive effort by government to ensure easy access by citizens. Thus, while publication requires active effort to bring information to peoples' attention, making it available merely implies that government has prepared the ground for access by individuals.[15] Today, both publication and making available often occur within the framework of the Internet. Explicit information on a homepage would typically be regarded as publishing, while a PDF-document deeply embedded in the structure of a

---

13 See Act 1969-06-19-53.

14 See http://www.odin.dep.no/jd/norsk/publ/hoeringsnotater/012041-080078/index-dok000-b-n-a.html The same amendment established the opportunity to publish various legal instruments voluntarily.

15 See Act 1999-01-15-2, Authorised Public Accountant Act (revisorloven), sections 3-5 and 3-7, last subsections.

web-site would probably be regarded as making information available. Nevertheless, in many instances there will be plenty of room for doubt as to where the boundary between these two categories should be drawn.

A *duty to produce information* implies an obligation to produce particular information material, but without the duty to actively distribute it. For instance, according to the Norwegian Environment Information Act, section 8, every relevant government agency is obliged to possess environmental information covering their areas of responsibility and function.[16] The obligation to maintain file records and correspondence lists etc., should probably also be classified under this category.

A *duty to actively inform* represents a technique for the distribution of information where government has to do more than make information available. In addition, it is obliged to take active measures to reach out to members of the general public. In Norway, local governments, for instance, have a general duty to actively inform their citizens of their activities, and generally prepare the ground for general access to government-held information.[17] In contrast to publication, actively informing is based on the premiss that there are specific addressees (individuals or groups).

A *duty to announce* differs from the duty to publish in the sense that an announcement contains only a reference to the existence of the information in question and where it may be obtained. This technique is used, for instance, to facilitate democratic debate regarding draft area development plans at county level.[18]

A *duty to notify citizens* is among the central provisions of both the PAA[19] and PDA.[20] The obligation to notify is motivated by situations where it is necessary to gain the attention of specific individuals in order to make them consider their own interests.

A *duty to provide guidance* implies an obligation to make an active evaluation of the extent to which individuals need to be informed of their rights and duties etc. The pendant to this obligation is the right to request guidance, see below. According to the Norwegian PAA, section 11, subsection 2, assessment of the need for guidance is to be carried out on the initiative of the government agency. Moreover, and of particular interest in the context of this article is the provision in section 6, subsection 2 of the PDA,

---

16 cf. Act 2003-05-09-31.

17 cf. Act 1992-09-25-107, Local Government Act section 4 (kommuneloven).

18 cf. Act 1985-06-14-77, Act Regarding Planning and Building, section 19-4 (plan og bygningsloven).

19 Section 16.

20 Sections 19 – 21.

referred to above, which establishes a duty to provide guidance regarding statutory rights to access information.

A *duty to give grounds for decisions* is among the basic rights to receive information, and is a particularly important element of the Administrative Procedure Act.[21] In some cases, individuals may have the right to request grounds beyond those that government agencies are obliged to give on their own initiative (see below).

b) Rights of individuals to obtain information

The *right to request access to meta information* concerns information that is often used to identify documents (see below). In other words, meta information can be regarded as the key to other and richer bodies of information. However, meta information may, in itself, be of interest because it reveals relations, points of contacts and various other structures. Thus, information in logbooks, case records, agendas etc. is often of great interest, irrespective of the underlying information. Meta information is usually identified in accordance with legal rules or other norms such as the National Archives Act and conventions regarding the contents of agendas.

The *right to request access to documents* is probably the most common way of creating openness within government and is a core element in freedom of information legislation. In Norway, the concept of "document" has developed from referring merely to a written piece of paper, to the all-embracing statutory definition: "a logically limited quantity of information stored on a medium which enables later reading, listening, presentation or transmission".[22] In order to specify which documents to access, a "specific case" must be identified, combining "document", "specific case" and the information of case records. A core of material, subject to information access, must be easily identifiable. However, accessible documents are not limited to those formally recorded as being part of a case, and an individual may have access to documents in a number of cases. Thus, a "specific case" is primarily the designation of a starting point and does not exclude any document that the individual may regard as relevant.

A document will always contain a variety of items of information, from specified and formalised types of information to that contained in factual prose, photographs, soundtracks etc. In other words, information may be expressed in ways that may make it difficult to determine in advance what should be regarded as one item of information. Nevertheless, exceptions

---

21 cf. sections 24 and 25.

22 In Norwegian: "logisk avgrenset informasjonsmengde som er lagret på et medium for senere lesing, lytting, fremvisning eller overføring", cf. AGI, section 3.

from access to documents may often comprise specific items of information, for instance personal or private information.

The *right to request access to specific types of information* may sometimes supplement or facilitate the right of access to documents. According to the PDA, section 18, subsection 1, everybody has the right to access information that provides a general description of how personal data is processed. Moreover, the right to access specific types of information may also confer the right to access certain types of information contained in otherwise inaccessible documents.[23]

The *right to receive guidance from a government agency* may either be of a general nature or linked to particular challenges, e.g. completing forms or acquiring knowledge of the contents of statutory or case law. This right is often universal, i.e., regardless of status, for example, as the party to a case.

The *right to request the grounds for decisions* supplements the obligation for government agencies to give grounds.[24] In Norway, such a right to obtain the grounds for decisions applies to specific fully automated decisions, in accordance with the PDA, section 22.

Finally, *the right of access to meetings of public decision-making bodies* implies the right to acquire transient information, for instance by attending meetings of central or local government bodies. In Norway, such rights exist within central and local government and within the court system. Rights to attend meetings at local government level may be accompanied by a duty to announce the event and to make the agenda publicly available.[25]

In sum, this categorisation of access rights indicates a variety of ways to create openness. From the viewpoint of the legislators, it would probably be useful to develop a "toolbox" for the design of access policies and provisions. The aim should be to break the broad "access rights" down into smaller, well-defined elements that could be instrumental in the formulation of precise and well-founded access provisions.

5. Putting access rights together

In principle, access rights should first and foremost be improved through statutory amendments, to result in a co-ordinated and fully comprehensive body of provisions. Realistically, such an objective lies, at best, in the rather

---

23 For instance, according to the PDA, data subjects have the right to access information concerning "security measures implemented in connection with the processing, insofar as such access does not prejudice security" (section 18, subsection 2, litra b).

24 See, for example, section 13, subsections 4 & 5 of the Environment Information Act.

25 cf., for instance, the Local Government Act, section 32.

distant future. As an alternative, each government agency may develop its own internal policy, placing various elements of access rights together and correcting deficiencies in access legislation. In this section, I will attempt to illustrate how a simple *access procedure* model could contribute.

To transform the categories presented in the previous section into more than a list, it would be reasonable to place each element into what could be regarded as a typical (yet simplified) *information access procedure*. I have defined the possible phases of such a procedure in the table below and placed each category from the list in one of phases. That I have only chosen one phase for each category is not meant to preclude the possibility that categories may occur in several phases. Indeed, "guidance", for instance, may be placed in several of the phases. However, I have presupposed that the placing of elements in the figure is simplified and typical, representing an adequate, albeit incomplete, representation of the information access procedure.

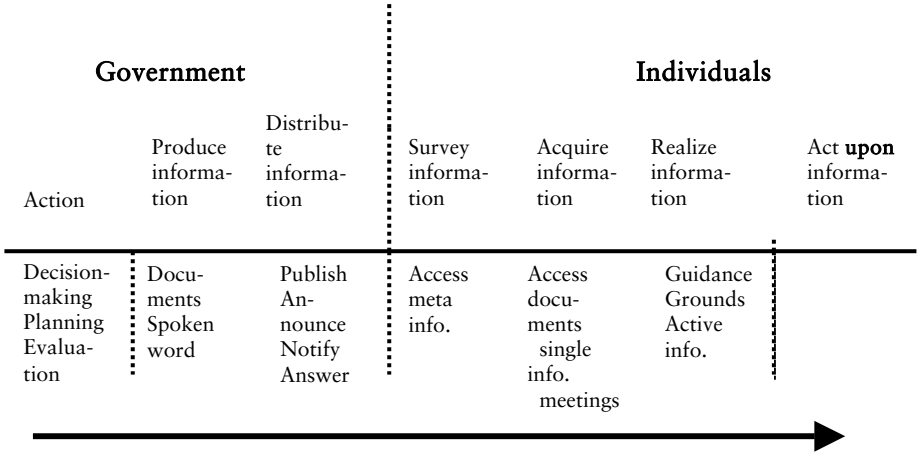


Table 2

The first three phases represent the government's responsibilities, i.e. where a government agency is the active party. "Action" represents occurrences of administrative and political action, such as decision-making, planning, evaluation of policies, exchange of information etc., i.e., processes that citizens may later find of interest and worthy of accessing information about. The second phase ("Produce information") represents situations where government produces information relating to an "action", either in a transient or

documented form . The third and last phase in the government's part of the process ("Distribute information") is where the government takes steps to ensure that the information concerning the action in question is made known to a wide or narrow circle of individuals.

During the next three phases of the procedure, the active party is individuals wanting access to government-held information. Government agencies must act in response to requests. The first typical step is to establish an overview of possible information objects to access ("Survey information").[26] Various types of meta information such as logbooks, case records and agendas may be used. Such information directly or indirectly discloses the information objects that are often the target of the whole information access process ("Acquire information"). Both meta and "target" information may be subject to scrutiny by citizens. However, I have assumed that case documents, items of information from filing systems, data bases etc., and occurrences and statements in meetings will, first and foremost, be regarded as target information, and thus the most important to acquire.

In the final phase of the procedure ("Understand information"), individuals deal with the challenge of interpreting and comprehending the information acquired. In doing so, individuals may need various types of general or individually oriented supplementary information or guidance, specific or general grounds for individual or general decisions etc.

Irrespective of how legislation is designed and the extent of statutory coordination (see above), it is important that government agencies make an effort to safeguard an appropriate level of information availability. To meet this challenge, a thorough analysis of the two phases that follow "Action", on the "government side" of the model above is required, i.e. "Produce information" and "Distribute information". Here, I will identify further elements linked to these phases and discuss how government may help to make access rights operative by developing an internal policy regarding access to government-held information.

Consideration of the production of information should start by identifying the government actions that are most likely to be relevant to the practise of access rights. If we extend the example presented in table 2 (above), "actions" may, for example, be stated as in table 3 below. The point here is not the comprehensiveness of the list, but the attempt to make a detailed subcategorisation of government actions, linked to particular main categories. The main categories are useful primarily to organise the list, while the intention is to employ subcategories in concrete policy-making and planning processes

---

[26] Even the government agency needs to survey the produced information. Thus, "survey" may also be placed on the government's side of the model.

(see below). It is certainly outside the scope of this article to discuss every one of the subcategories in the table, and I will limit myself to comment briefly on a couple of points.

Performance of processes
Statutory
Budgetary
Planning
Projects
Individual cases
etc.
Adoption of structures and systems
Physical organisation
Formal organisation
Information systems
etc.
Social event(s)
Parliamentary meetings
Conferences
etc.
Miscellaneous

Table 3

Access to information connected to statutory provisions is of great importance for many groups in society. Among the statutory instruments, regulations pursuant to Parliamentary acts e.g. issued by the Government or ministry are key. In Norway, preparatory work and draft legislation are generally regarded as important legal sources, in particular as a guide to the interpretation of new acts. Regulations are not often accompanied by the preparatory work, by and large leaving the reader to interpret the text itself. Thus, taking into consideration the performance of statutory processes (see table 3 above) and the question concerning production of accessible information, a key question for a ministry could for instance be: which documents related to new legislation should be produced and made accessible? Should, for instance, documentation describing the general and/or particular grounds for the legislation and/or each provision of the legislation be produced? In the next phase (in accordance with table 3 above), a further question should be: how should the relevant documents be distributed? Should they be published, announced, notified, or should the relevant government agency merely respond to requests to access the documents?

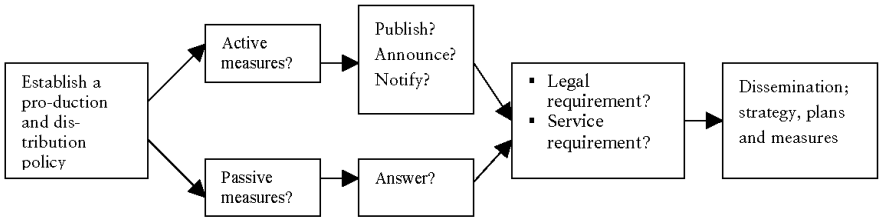


Figure 1

Another example concerns information linked to what I have cheerfully termed "social events" (see table 3 above), but which, in fact, designate the process whereby individuals (officials, politicians etc.) meet to take administrative or political actions. Such events may be of interest to citizens wishing some form of information access, for example the meetings of a decision-making body such as the Board of Social Affairs in a local government. According to my approach, the Board would first map the production of information in their meetings, as well as the types of document generated (agenda, spoken words, statements of cases, proposed decision, minutes etc.). The next phase would be to consider how the information should be distributed, i.e., which of the techniques identified in section 4 above, if any, should be applied. Who, for example, should have access to the meeting itself (and the spoken word), and in what form should minutes from the meeting be accessible (published on web-site only, announced and published, copies provided on request, etc.)?

Obviously, the subcategories in table 3 above will often be linked together. For example, a meeting of an administrative body may be called in order to make decisions, implying that questions regarding access to information concerning the meeting and other parts of the total decision-making process must be seen as a whole. In table 4 below, I have used a small example to illustrate such a combination, and have, in addition, applied some of the other categories presented earlier in this article. My intention is to illustrate how the various categories may be used to approach questions of access in a systematic manner which may, in turn, be employed to develop strategies, plans and specific measures to address access rights in a more satisfactory way than in current legislation.

Meta information	correspondence list		agenda						correspondence list
Transient information		telephone calls from parties				spoken word (meeting)			
Documented information	letter from parties	sound recordings		statements of cases	proposed decisions	video recording	minutes	decision	letters to parties
Means of access	on request	on request	publish + announce	on request	on request	accessible via the Internet	publish	on request	on request

Table 4

In table 4, the last row contains examples of the types of access methods that may be employed. A crucial question for government agencies concerns which of the two communicating parties (government agency or citizen) should initially play the active role? From the government agency's point of view, the question is to what extent the strategy etc. should contain active and passive elements, and what the interplay between these two groups of elements should be. This division corresponds with the division between the duties of government and citizens' rights. Based on the overview described in section 4, different measures may be roughly classified in accordance with this division:

Active distribution (duties of government agencies)	**Passive distribution** (rights of citizens)
publish	access meta information
make information available	access documents
announce	access specific types of information
produce information	access to meetings in government bodies
inform actively	guidance from government agencies
notify	grounds for decisions
provide guidance	
give grounds for decisions	

Table 5

The first step in the distributing information phase would be to identify any legal obligation of the government agency in question to actively distribute information and any legal right of citizens (or groups of citizens) to obtain information from the agency. The next step would be to consider whether or not the agency should provide services to citizens additional to those mandated by statutory rights and duties, see figure 1 above.

In Norway, the general principle of additional access to information is recognised, implying that more information may be provided than that guaranteed by statutory law, provided that no requirements for secrecy hinder such access. In other words, statutory access rights represent a minimum standard and can be exceeded at the government's discretion. Of course, certain additional access initiatives may only be decided on a case-by-case basis, while others may be decided and fully established beforehand. General policies and procedures regarding active information vis-à-vis parties or data subjects may, for instance, be established independently of concrete cases. At the same time, the extent to which active and passive measures might interplay with each other should be exposed and considered. The obvious example is that the right to receive guidance and the duty to provide guidance are closely related. However, even less complimentary relationships should be examined, for instance the connection between notification and the volume and nature of access requirements. The aim of this process should be to find the right balance between "active" and "passive" access strategies, and, furthermore, identify a corresponding and balanced set of measures. A systematic approach similar to that outlined above may contribute to a carefully considered information strategy that also provides the basis for evaluation and a dynamic and adaptive endeavour to secure satisfactory open government.

6. Rights and usability

Individual rights have been reinforced in the amended Norwegian data protection legislation, the underlying assumption being that, with the PDA, individuals will play an active part in the effort to achieve an acceptable level of data protection. Moreover, a Norwegian expert committee has proposed an amendment to the AGI, extending individuals' rights to access documents, particularly those in the "grey" zone between government and private agencies. However, giving citizens legal rights is not in itself sufficient to improve access. In addition, how and to what extent data subjects may be helped or encouraged to maintain their interest in exercising their statutory rights is crucial.

In recent discussion concerning the AGI, two of the main themes have been, a) a discussion about how to improve openness through statutory amendments, and, b) the potential for increasing the efficiency of existing access rights by means of information technology. Concerning the second theme, the premise is that the legislation may be sufficient, even if its practise deviates from political objectives. In other words, what might be deficient are the organisational and practical arrangements necessary for citizens to exploit the full potential of existing legislation. Seen from this perspective, an impor-

tant question regarding the implementation of access legislation is the extent to which existing legislation is accompanied by adequate enabling initiatives, i.e. technological and other measures that make it comparatively simple for citizens to exercise their statutory rights. In any case, there is obviously a significant difference between "anonymous" formal rights on the statute book and a "materialised right" in the shape of a publicly available computerised tool, accessible, for example, via the Internet.

In Norway, the Section for Information Technology and Administrative Systems (SITAS) at the University of Oslo has developed a general, free of charge, internet based routine in order to make enable some of the core access rights of the PDA.[27] The function of the tool is threefold: firstly, to offer legal information services by making available the relevant statutes, together with intelligible, well-grounded explanations and practical examples; secondly, to generate access requests (neatly arranged, with references to legal bases etc.) and, thirdly, to generate advice to the recipients of requests (the "controllers") regarding how the requests should be processed.

My general point here is that access rights in the form of statutory and associated explanatory texts, are insufficient to create conditions where access rights have any real effects for more than a small number of citizens. To increase the usability of such rights, they must be transformed into tools that perform the functions the access provisions describe. In other words, the usefulness of access rights should, as far as possible, be independent of an individual's ability to identify, access, interpret and act upon formal legislation. Rights should, as far as possible, be brought down to the "ground level" of peoples' everyday life, with no or very low thresholds to exceed.

One obvious objection to such an easy, populist approach is the danger of generating too much discussion and disturbance, as a consequence of a large volume of access requests. In my view, there are at least three weighty replies to such an admonition. Firstly, there is, in my view, little reason to fear that the extent to which people exercise their access rights will change dramatically as a result of improved usability. As the figures referred to in the next section illustrate, the use of access rights is minimal and, although it may increase, will probably not exceed a moderate level. Secondly, to the extent that use of access rights will increase, there are a number of obvious strategies to reduce the attendant costs. It may, for instance, be more cost-effective to change from a passive to an active approach: publishing information once rather than answering 20 individual requests. Moreover, just as the usability of rights may increase if internet based tools were available, the administra-

---

[27] The routine has been further developed in collaboration with the EC/IAP sponsored SAFT project (Safety, Awareness, Facts and Tools) and the Norwegian Board of Education [Læringssenteret].

tive costs associated with providing access may be reduced if tools were developed to assist government agencies in processing requests. Thirdly, and most importantly, there are costs associated with the creation and maintenance of an open society. Such increased costs should, to a necessary extent, be both expected and accepted.

7. Taking access rights seriously

In a special Eurobarometer carried out in the autumn of 2003, only 32% of citizens in the (at the time) 15 EU countries had heard of laws that, for example, granted individuals access to their personal data held by others. The results ranged from 13% in Greece to 53% in Italy, with Sweden and Denmark as low as 26% and 23% respectively.[28] Norwegian citizens did not take part in the survey, but there is no reason to believe that the result would have deviated significantly from the average figures. In 2002, European companies were asked about their experience with regard to access requests. Average figures showed that almost half the respondents (49%) had received less than 10 access requests in the course of 2002, while 14% indicated that their company had received between 10 and 50 requests. Only 8% of respondents stated that they had received 50 access requests or more. The average for companies never having received access requests was 23%, ranging from 7% in Germany to 58% in Italy.[29] On a smaller scale, a survey carried out in Norway by SITAS revealed that a mere 42% of the access requests (n=93) submitted by pupils at a Norwegian secondary school received a response within 30 days (the deadline defined in the PDA).[30]The data available concerning data protection law seems to paint a rather discouraging picture of somewhat ignorant and passive citizens. Furthermore, more than half of the few who do know how to make use of their rights have been disappointed. Viewed scientifically, such figures cannot, of course, be combined in such an offhand manner. Nonetheless, the figures should be taken as an indication that access rights in accordance with European data protection legislation are of rather modest significance.

---

28 See Special Eurobarometer 196, question 33 a.2, Internet: http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_data_protection.pdf.

29 See EOS Gallup Europe - FLASH EB N°147 «Data protection in the European Union » - Report p. 47, question 11, Internet: http://europa.eu.int/comm/public_opinion/flash/fl147_data_protect.pdf.

30 The final report is under preparation, for further information please contact Section for Information Technology and Administrative Systems [Avdeling for forvaltningsinformatikk], University of Oslo.

Indeed, figures concerning data protection may not provide a basis for generalisations regarding the situation for access rights pursuant to other legislation. However, in my view, there is reason to be concerned about a trend where access rights, for others than representatives of the press, become symbols of good intentions rather than reality for the ordinary citizen. Taking access rights seriously implies effort to contribute both to a high level of public knowledge, easy to use access rights, and responding effectively when individuals actually exercise their rights. Taking access rights seriously is about making access rights operative.

4 WHY IS THE SAME TECHNOLOGY USED DIFFERENTLY ACROSS AN ORGANISATION

A study of the introduction of a case processing system in a Norwegian municipality

By
Arild Jansen…
Section for Information Technology and Administrative Systems (SITAS)
Faculty of Law, University of Oslo, P.O. Box 6706, Oslo, Norway
arild.jansen@jus.uio.no
http://www.jus.uio.no/iri/om_iri/folk/ansatte/jansen.html

…and Terje Nes
The National Archives of Norway
E-post: terje.nes@riksarkivaren.dep.no

Summary

This paper reports from an evaluation of the implementation and use of an integrated archiving and case processing system in a Norwegian municipality. The implementation and adaptation of this system was part of a strategy for reorganising the municipality from a traditional multilevel bureaucratic model towards a network oriented organisation based on two levels.

Our analysis clearly indicates that various groups in the organization enact different technology-in-use with the same system across various context and practices. At the same time, it is also revealed how these structures have influenced the characteristics of the systems in the way it is being adopted and used in different parts of the organisation. The paper offers an illustration of how Orlikowskis extension to structuration theory offers a fruitful way of explaining the variations in how the same systems is being used across the organisation when introducing a new IT-system in a large organization. Thus, we believe that Orlikowskis notion of technology-in-practice provides a fruitful framework for evaluating IT implementations in organisations.

Key words: Evaluation of system use, eGovernment, technology-in-practise, theory of structuration, IS adoption,

1. Introduction

Norwegian municipalities are under strong pressure to become more effective and service-oriented. Therefore, many of them are being reorganised from a typical bureaucratic model to a two-level network oriented organisation, in which e.g. the case workers are given much more responsibility for carrying out their tasks, including doing the administrative work that were typically done by the secretaries and personnel responsible for archiving etc. Modern ICT systems play an ever more important role in such reorganisations. Typical systems that integrate archiving and case processing are provided to support task that previously were done manually.

This paper reports from a study[1] of the introduction of one such system, called *Ephorte*[2] in a middle-sized Norwegian municipality in 2001-2002. It is being used by archiving personnel, case processing personnel and managers. This system is frequently installed in number of organisation in both public and private sector, and it complies with the Norwegian standard for archiving routines. One experienced, however, that the system was not used as expected in many parts of the organisation. The paper aims at explaining why system is not being used as anticipated, by applying Giddens' structuration theory (Giddens 1984), as extended by Orlikowski (Orlikowski 1992, 2000).

The paper is structured as follows. Chapter 2 and 3 gives the theoretical framework and the description of the methodological approach. In chapter 4 we present the empirical data, followed by our analysis and the final conclusions.

2. A Structurational model of Technology

Giddens (1979, 1984) has among others challenged the long-standing opposition in the social sciences between the subjective and objective dimensions of social reality, and proposes an alternative meta-theory which incorporates both dimensions. Giddens theory of structuration offers a solution to the dilemma of choosing between subjective and objective, between actors and structures, in that it recognizes that human actions are enabled and constrained by structures, yet that these structures are the result of previous actions. In his framework, structural properties consist of the rules and resources that human agents use in their everyday interaction. These rules and

---

1 This study is reported in the master thesis of Terje Nes: "Introduction and use of Ephorte in Lier Municipality" by Terje Nes, Department of informatics, University of Oslo, (Nes, 2003)

2 *Ephorte* is standard software system developed by *Ergo Ephorma*, a Norwegian software house.

resources mediate human actions, while at the same time they are reaffirmed through being used by human actors (Giddens, in Orlikowski 1992, p 404). Giddens notes (1984, p 22) *"All social actors, all human being are highly learned in respect to knowledge which they possess and apply, in the production and reproduction of day-to-day social encounters".*

Through the regular actions of knowledgeable and reflexive actions, patterns of interaction become established as standardised practices in organisations, e.g. ways of manufacturing a products etc. Over time, habitual use of such practices becomes institutionalised, forming the structural properties of organisations. These institutionalised properties (structures) are drawn on by humans in their ongoing interactions (agency), even as such use, in turn reinforces the institutionalised properties, the *duality of structure.* In this way, the individuals both shape and are being shaped by the structures.

While the structurational theory as such does not address the issue of technology, Orlikowski (1992) has developed a structurational theory of technology which is further extended in the paper "Using Technology and Constituting structure: A Practical lens for Studying Technology in Organizations" (Orlikowski 2000). She proposes a practice-oriented understanding of the recursive interaction between people, technologies and social action. Crucial in this approach is the understanding of structure, the set of rules and resources instantiated in recurrent social practice. Elements of technology, as in our case would be e.g. archiving standards, working routines, document templates etc. is not structure in itself, they become so when they

> *[..] are routinely mobilised in use that we can say that they "structure" human action, and in this way they become implicated as rules and resources in the constitution of a particular recurrent social practice (Orlikowski, 2000, p 406). She continues "the myriads of software packages [..] until such time as these are actually used in some ongoing human action- they are at best, potential structuring elements, and at worst, unexplored, forgotten, or rejected bits of program code"*

According to this view technology does not have embodied structures. As a consequence, she says : "rather than starting with the technology and examining how actors appropriate its embodied structures, this view starts with human action and examine how it enacts emergent structures through recurrent interaction with the technology at hand." Thus, we have to analyse how structure of technology use are constituted recursively as human regularly interact with certain properties of a technology and thus shape the set of rules and resources that serve to shape their interaction.

Structuring of technology-in-practice

Giddens (1984) proposed the notion of structure as the set of enacted rules and resources that mediate social action through three dimensions of modality: facility, norms and interpretative schemes. When people use a technology, they draw on their tacit and explicit knowledge, the facilities available to them and the norm that inform their ongoing practices. In doing so, they recursively instantiate and thus reconstitute the rules and resources that structure their social action. Orlikowski (2002) states that"*because technology in practice is a kind of structure, the same recursive constitution applies here to*". When people uses a technology, they draw on the properties comprising the technological artefact – those provided by its constituent materiality, those inscribed by the designers, and those added on by users through previous interactions. This may be illustrated in this way:

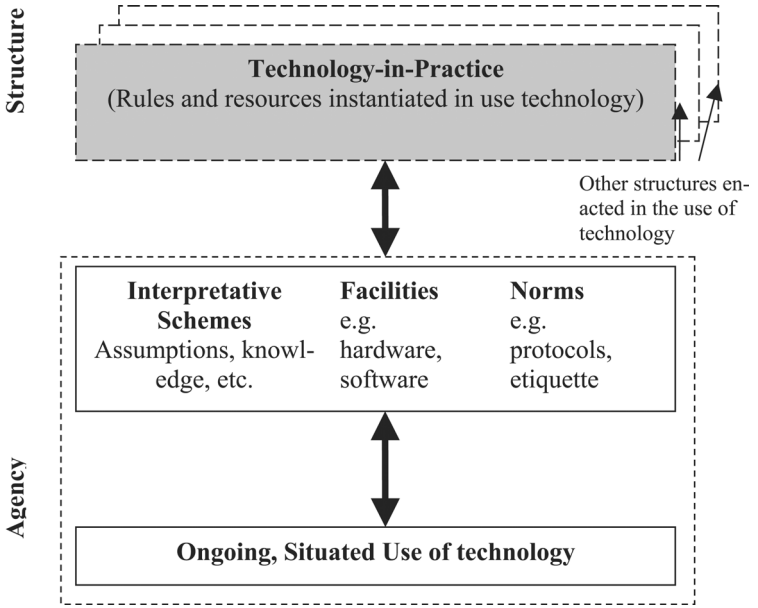


Figure 1: Enactment of Technology-in-Practice (from Orlikowski, 2000, p 410)

Figure 1 shows how our use of technology is structured based on experiences, knowledge, assumptions, behaviour, power relations, and norms along with the technology itself. A group of users that are involved in the same type of work enacts similar technology-in-practice, where through common training

sessions, shared socialisation, comparable job experience etc., users come to engage with a technology in similar ways. Technologies-in-practice can be and are changed as actors experience changes in awareness, knowledge, power, motivation, circumstances, and in the technology itself. They are changed through the same process that all social structures are changed – through human action. Orlikowski emphasizes that technologies are never fully stabilised or complete, even though we may choose to treat them as fixed black boxes for a period of time. As people enact modified technologies-in-practice they also change the facilities, norms and interpretative schemes used in their use of the technology. She states that users always have the option, at any moment and within existing condition and materials, to do otherwise.

3. Research approach

The aim of this field research project was to study how Ephorte was used in an organisation, both the range of use and for what type of tasks. We would investigate what type of attitudes and understanding the different user communities had related to the system. The main research questions have been:

i) Why was not Ephorte used to the extent it was anticipated by the management
ii) Why did the various user groups use the system differently

These research questions required a combination of qualitative and quantitative data through triangulation (see e.g. Jacobsen 2000). The empirical data was collected over a period of 18 months, consisting of three phases. The first phase included of introductory, unstructured interviews and conversations with key personnel in the ICT department along with other managers. In the second phase, we conducted a survey where a questionnaire was mailed to all anticipated users of the system. Of estimated about 200 users, we got 115 responses. The aim was to get a broad picture of the use of Ephorte, as e.g. the user experiences, how the training had been, experiences, specific problems with its use etc. We did, however, learn that the questionnaire had some weaknesses in its design; e.g. that it did not take into account the substantial variety in use of the system. Accordingly, the data that was collected did not provide sufficient information on why there were these variations in usage patterns.

The third phase consisted of follow-up, unstructured interviews with 8 key users of Ephorte. In these interviews, the users were invited to express their more detailed experiences from using the system. Insight gained in the first of these interviews was used in the following interviews, in order to

check whether e.g. attitudes we found among some users was shared by others. Along with these interviews, we participated in meeting and as observers on training courses.

4. The Introduction of Ephorte in the organisation

Lier municipality has 1400 employees, of those about 200 clerks and other case processors are assumed to be users of Ephorte. Some of these would use Ephorte on a daily basis while others are rather infrequent users. The introduction of Ephorte was an integral part of the reorganisation of the municipality, from a rather bureaucratic organisation consisting of 4 hierarchical levels to a more network-like structure having only two levels and 54 separate organisational units. One implication was that the number and size of central support functions was rather dramatically reduced, as e.g. the archiving office. Accordingly, the clerks and other case workers had to do a lot of administrative routines themselves, as e.g. the archiving of incoming mail. The introduction of Ephorte was thus seen as an important mean for making the clerical work simpler and more efficient.

The archiving unit became part of the ICT department, including only two employees, and none of them do have professional background within this area[3]. The municipality has to day a partly centralised archive, supporting only those units that are located in the city hall building. Most units are therefore responsible for taking care of the recording and archiving themselves. The way they carry out these tasks may vary substantially.

The principle of case processing in the municipality is so called *completed case processing,* which implies that the clerk that in the first place receives the case is then responsible for all phases in the processing of the case until it is completed. Furthermore, the processing should be done on the lowest possible level in the organisation. The responsible clerk has to make sure that every relevant factor is included in the decision making process. This way of working implies that the clerk have to involve persons from other departments and from various levels in the organisation. Research has shown that this way of processing a case is more flexible and often more efficient (Bukve 1997).

The archiving function is strictly regulated by Norwegian laws, in that every public institution, including municipalities are obliged to record every incoming and outgoing letter according to certain standards. A specific standard, cur-

[3] During the first phase of this project, the head of this unit was a professional archiving person, but she quit during this process, partly as a result of the lack of support from the management

rently Noark-4[4] provides a detailed specification of functional requirements for electronic recordkeeping systems used in public administration in Norway. A major issue in Noark-4 has been to facilitate the receipt and filing of any e-mail that makes up or contains administration documents. The Noark-4 includes several layers of standards, both basic obligatory requirements to be met by all systems, and additional, more advanced functions.

The implementation process

The acquisition and implementation of Ephorte was defined as a project within an overall ICT strategy for the whole organisation. Ephorte was chosen among other reason because it fully complies with the Noark standard, and it was even at that time used by a number of organisations[5] in private and public sector. The system has included functions for document flow and case processing, and is intended to be used by archiving personnel, clerks and case workers and even managers. Ephorte has a number of different modules that may optionally be installed. Each individual implementation of the system has to be specifically configured and parameterised. One important part of this work is to define roles that must be given to each authorised user of the system. In the implementation of Ephorte in this organisation not all modules were implemented, and they do not use the system as a complete archiving system.

The implementation project was initiated early 2001, and was headed by the leader of the archive office. The project group was recruited by user representatives from various departments, and they should actively participate in the configuring and tailoring of the system. However, most of them did not fulfil their obligations, which then were carried out by the project leader, running the danger that the parameter setting, e.g. defining roles, templates, schemes etc. did not fit the need of the individual users. Furthermore, the first consultant from the vendor did not fully understand the specific organisational structure of the municipality, resulting in that the system configuration in the first place was wrong. This consultant was later on replaced, and the system configuration was substantially improved, but it caused a lot of problems for the first users of the system.

An important part of the implementation process is user training. In our case, the training was intended to be taken care of by local *super-users*, which were users from the different units in the organisation. One reason for this was that the limited budget for this project did not allow for buying rather expensive training courses from the software company. As important was the need

---

4 Noark – Norwegian recording and archiving standard

5 To day it is used by close to 100 organizations in public and private sector.

for building-up user competence locally in the individual user communities. These super-users were supposed to know the specific routines for case processing locally, which however not always was the case. One specific problem was that some of these super-users had quite different tasks and roles in the local unit compared to the clerks they were going to train. According, they were not able to provide sufficient support for changing working routines in order to make work more efficient. Another problem was that the courses offered by the vendor were not satisfactory, having the consequence that the super-users were not as competent as they were supposed to be. Accordingly, many case workers expressed clearly that the training had been inadequate.

How is the system used?

About 200 users have access to Ephorte, including clerks and other professionals, managers, secretaries and some other. In addition some of the politicians may use the system, but they are not included in this study. Figure 2 below shows that out of the 115 respondents that turned in the questionnaire, we found that 20% answered that they did not use the system at all[6]. About the same number of users says that they use the system on a daily basis.

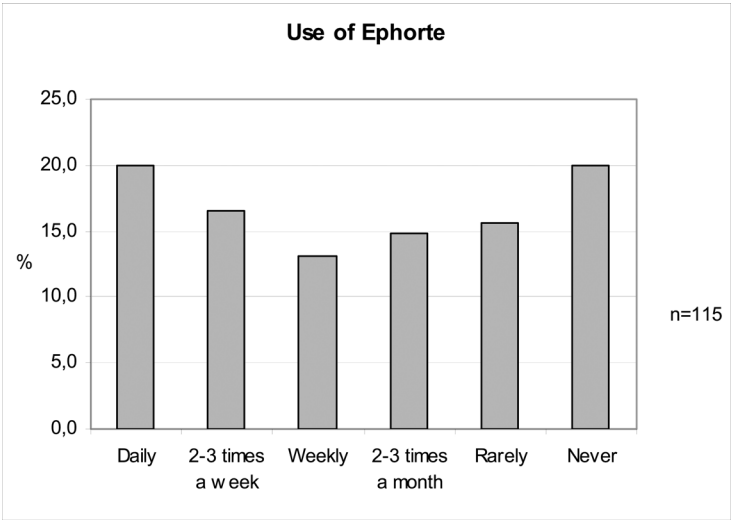


Figure 2: Use of Ephorte

[6] These data were collected January 2003.

Figure 3 shows what Ephorte are being used for. Of the 88 respondents that were active users, a majority (83 % of them) answered that they used it for case processing, even the managers said so. Less that 20% used it for writing letter, exchange of information, statistic purpose and others (Note: The respondents were allowed to give more than one answer).

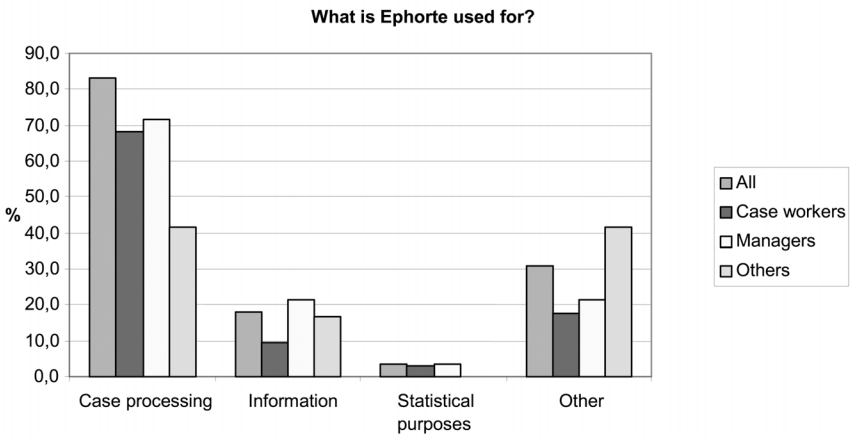


Figure 3: What is Ephorte used for

Analysis

The system is developed by people being familiar with the public sector, and one particular developer have in the past been working active with archiving work, and even participating in the specification of the Noark-4 standard. When developing the system, they used their interpretative schemes and knowledge about how such work are being conducted in public organisations. This understanding of the legal framework, work routines along with their previous work experience in this field strongly influenced the way Ephorte was developed. Thus, the first version of Ephorte was developed strictly according to the Noark-4 specifications. They even applied the data model that was outlined in the description.

However, it turned out that understanding of working routines and responsibilities did not comply with the way such work was organised in a local municipality. There are also significant variations across one organisation. The range and type of tasks among different user groups varied a lot, and they accordingly did use the systems in quite different ways. When ana-

lysing the data we found several distinct patterns which we believe can be attributed to such differences. These *technology-in-practices* discussed below should not been seen as exhaustively characterising what the users did with the system at their work place. These are however, patterns that have been identified from data on a limited number of users in the organisation. Below we will present two structures of technology-in-practice, which must be seen as simplifications.

Limited use of the system-in-practice

The structure *limited-use* of Ephorte, see figure 4 was enacted by users that experienced that the system did not make their work more efficient. They regarded Ephorte as an important mean for the organisation as a whole, but was not able to see how the system could help them, e.g. in finding correct information, make relevant documents available for others, or in collaboration with others, etc. As one user said:

> *If one wishes more advanced users and users that prefer to use the system, one should have provided better and more adequate training. One issue is to master the technical aspects of system, but as important are the coding principles (principles for archiving) and how one can utilise the potentials that are inherent in the technical solutions [Case worker, February 2003].*

This answer is typical for the group of users that did not use the system for the tasks they were supposed to. Moreover, many of the users found the system difficult due to its strong basis in the record-keeping and archiving tradition. The terminology, screen layout etc. which was build in due to the developers interpretative schemes and understanding of how work should be carried out, appeared to be a limiting factor for how it was conceived by the users. As a consequence, when the user's interaction with the system was based on limited and inadequate understanding, this may contribute to enact the structure *limited-use*. In there current use of the system, they established user habits (also bad habits) and facilities as e.g. templates, that influences how the system became used. E.g., when the users do not utilise the various functions that the system offers, they will not gain sufficient knowledge to start using such function in a later stage, but rather continue using the system in a limited way. In the figure below we have summarised the most important factors resulting in this structure.

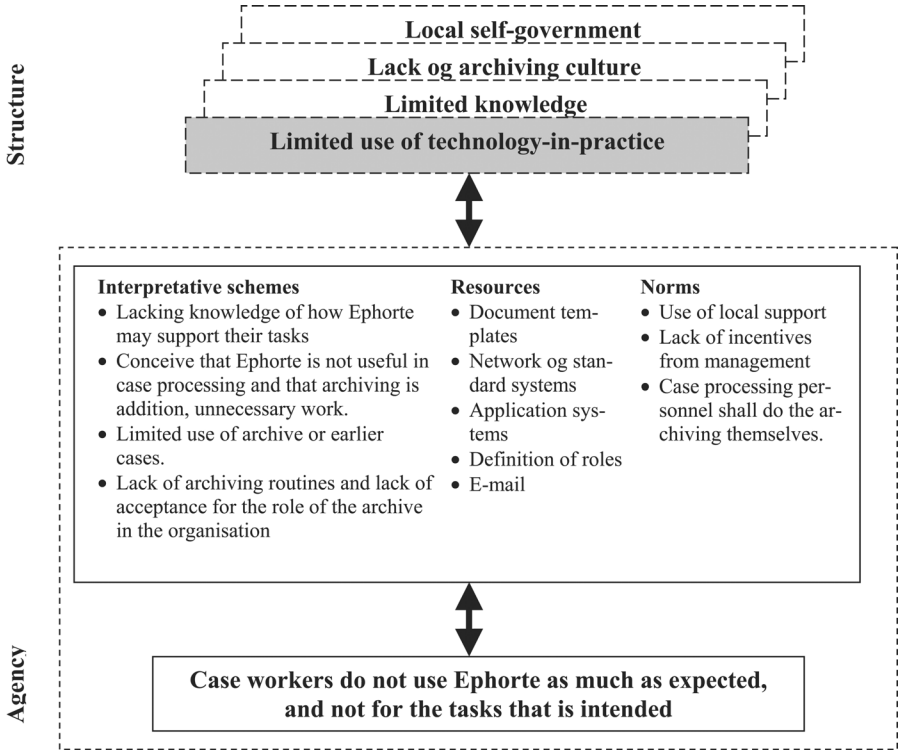


Figure 4: Limited-Use in practice of the system enacted by groups of case workers

It is, however, possible to break this pattern. One way is to participate in new, more adequate training courses. In cooperation with the chief archiving manager, it was developed new routines, document templates and better documentation that can help the case workers to benefit better from the system. Hopefully, this will weaken the limited-use structure.

Understanding of the role of case workers

The way Lier municipality practices "completed case processing" is institutionalized in case processing manuals[7], and these documents represent the structural characteristics that becomes apparent through human agency. The case workers do have their own understanding of what the role as case work-

[7] These documents are: *Fullført saksbehandling i Lier* (Completed case processing in Lier) and the user manual *Saksbehandlingsrutiner i Lier* (Case processing routines in Lier).

ers implies. A quite common view was that (and still are) that the archiving procedures is not their responsibility, but by the secretaries or the central archiving office. The tasks of case workers are to complete the cases and that should not include record incoming mail etc. As one user states:

> *Archive and so forth is not my field. [..] Whether one deals with economy or planning activities, one does not think about how the archive works, no reason for that. Rather the opposite, it is too much to be asked for. The archive should be viewed as a mean for us, and that it is understandable and fairly simple to use. One needs to have an archive office that can support the work we do and that it is expected to do. [Case worker, February 2003]*

The journal keeping was conceived as a task that one does if one have to, and is seen as extra work that is of no use for the case worker. However, the reorganizing process required that the case workers did a lot of office work themselves. This is a norm they have to comply to, but at the same time do many case workers experience/ feel lack of support and even pressure for this type of work. As such norms are not felt as sufficient strong, they will continue to do it their own way.

A number of case workers practice a non-standard way of processing the cases, including a lot of human judgments. The work is not following predefined routines, information and experiences from old cases are often of no help. They do not frequently collaborate with other clerks. In such cases, Ephorte is not seen as to be of any substantial help.

Lier municipality did not have any common arching plan[8]. The implication was that one has not institutionalised any practice regarding archiving work and made this available for the employees that would need it, and accordingly the way such work is done may vary considerable. One is thus running the danger that the quality of the archive is not satisfactory. Both the previous and at that time present chief of archive department felt that this work did not have any priority in the organisation. In current work practice, it is accepted that cases are not archived in a proper way. While the old organisational structure included local archiving personnel, the new model was based on small central archiving office combined with the presumption that case workers took care of such tasks in appropriate ways. As we have seen, this was in many user communities not the case. And the new system did not improve this situation.

---

[8] Archiving plan (arkiv plan in Norwegian) is requirement from the National Archives.

Usefulness and quality in work

However, there were several groups of case workers that used Ephorte as intended. They found the system very useful that improved the quality and efficiency of the work. It helped them finding information, and supported complete case processing. Access to relevant information is dependent on a well functioning archive having updated information This is particular the case for those being involved in more standardised case processing, where they often have to look at previous cases. The search facilities in the system are important, proving relevant and updated information when necessary. These case workers clearly saw the use of the system, and at the same time the necessity to keep it updated.

Furthermore, standardised case processing is characterised by that tasks are following similar routines most times, and that decision making are following well-defined procedures. In such cases, well developed document templates will simplify the work considerably, in that can apply standard references to rules and regulations. Also in work involving complicated agreements and contracts, such facilities were seen as extremely helpful.

Case workers involved in these types of work felt that Ephorte was very useful, and that it supported completed case processing in a constructive way. The way the collect information from previous cases, and exchange documents and viewpoints across departments in the organisation were well appreciated:

> *It is much easier to achieve completed case processing when the case processing writes down the arguments he is responsible for, directly into the document. It works excellent! [Case worker, February 2003]*

When one uses the system based on these preconditions, this understanding is likely to be reinforced by recurrent use. There was no need for pressure from the management to use it.

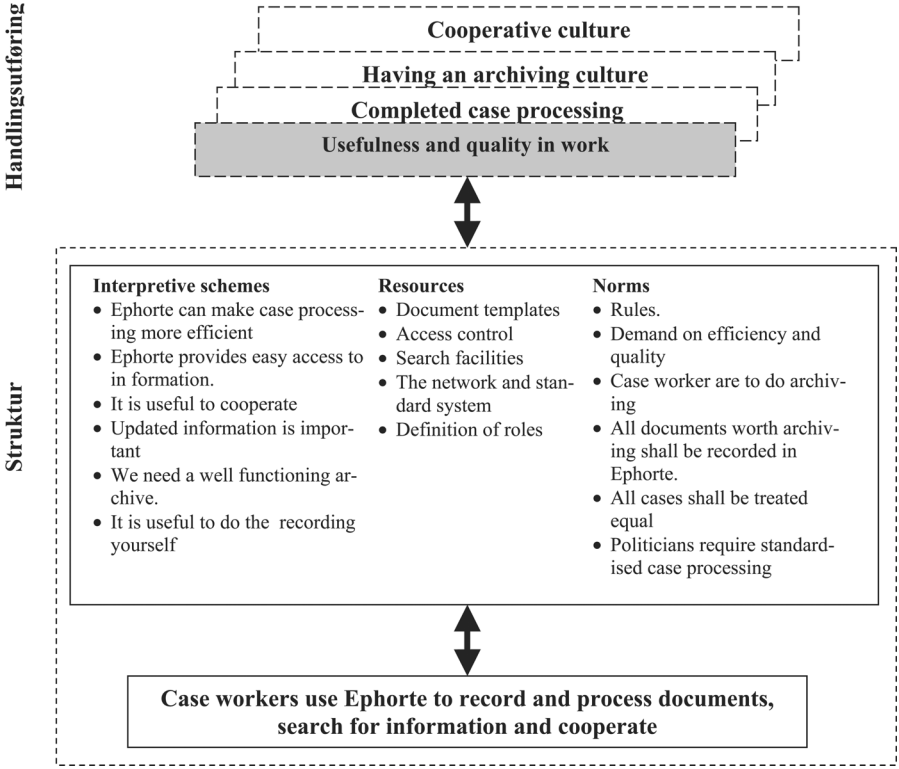


Figure 5 – Enactment of usefulness and quality technology-in-practice

5. Conclusion

In this paper, we have applied Orlikowskis extensions to Giddens structuration theory, where technology structures not are seen as embodied in a given technical artefact, in our case an application software system, but as enacted by the recurrent social practices of a group of users. We have focused on how various users groups used the system differently, and how their use is structured by the rules, that are their established working practices and the resources or facilities available. In the short version presented in this paper we have selected two sort of "idealised" patterns of use, which we believe illustrates that a number of factors influences how the system is used in daily work. These were, among other factors their own view on the type of work they are supposed do, their view on collaboration and sharing information

and knowledge, how they feel that the system may support their work, the lack a archiving culture along with more "usual" factors as lack of adequate training, inadequate configuration of the system, poor user support, technical problems and so forth.

Many of these factors could rather easily have been identified by traditional evaluation of implementation and use of information systems. However, we feel that the strength of this approach is its capability of describing the complexity in a rather understandable way. We have been able to see how individual actions and institutional structures relate to each other. Furthermore, this analytical framework may also be helpful in order to change existing structures. Even though that enacted structures of system use tend to be recurrent, they are not embodied in the system. Thus, it is possible to modify the institutional, interpretive as well as technical conditions that influences usage pattern. In our case, that could e.g. be to strengthen the archiving culture and the support for such work, to provide incentives for more collaboration, offer better training programs and so forth.

We believe our study has shown the strength of combining qualitative and quantitative approach in research, however done in a proper way. Our evaluation revealed weaknesses in the data collected in early phases of the study, which had to be supplemented in the later stages. Our findings should thus be verified by another quantitative study, which so far is not done.

References

Bukve, O. (1997): "Kommunal forvaltning og planlegging", Samlaget. Oslo. 3. utg.

Giddens, A. (1979): "Central Problems in social theory: Action, structure and contradiction in social analysis" Macmillan, London.

Giddens, A. (1984):"The constitution of society: Outline of the theory of structuration'' Policy Press, Cambridge.

Jacobsen, D. I. (2000): "Hvordan gjennomføre undersøkelser. Innføring i samfunnsvitenskapelig metode", Kristiansand, Høyskoleforlaget AS.

Nes, T. (2003): "Innføring og bruk av arkiv- og saksbehandlingssystemet Ephorte i Lier kommune. Ein analyse med utgangspunkt i struktureringsteori", Hovudfagsoppgåve, Institutt for Informatikk, Universitetet i Oslo, 2003

Orlikowski, W.J. (1992): "The duality of technology: rethinking the concept of technology in organizations," Organization Science, vol. 3 no. 3 (Aug. 1992), pp. 398-427

Orlikowski, W.J. (2000): "Using Technology and Constituting Structures: A practice lens for studying technology in organizations", Organization Science, Vol. 11, No, 4 (Juli - August 2000), pp. 404-428

Orlikowski, W. J. and D. C. Gash (1994): "Technological frames: making sense of information technology in organizations". ACM Transactions on Information Systems (TOIS), Vol.12 No.2, pp.174-207, 1994

Orlikowski, W.J. and D. Robey (1991): "Information Technology and the Structuring of organizations", Information Systems Research, Vol. 2, No. 2, pp. 143-169, 1991.

Walsham, G. and C. Han (1991): "Structuration Theory and Information Systems Research", *Journal of Applied Systems Analysis*, Vol. 7, pp. 77-85.

5 ELECTRONIC AGENTS: SPIES, LIES AND VILLAINS IN THE ONLINE WORLD?[1]

By Emily M. Weitzenböck

This paper examines some of the threats that may arise because of the increased deployment of autonomous software agents and highlights some recent legal developments in Europe in three fields: privacy and data protection, cybercrime and unfair competition. It first discusses the issue of surveillance and interception of data communication by electronic agents and the extent to which this is in breach of the Directive on privacy and electronic communications, and then looks at the elements of the offences of illegal access and unlawful interception of data proscribed by the Convention on Cybercrime. Finally, it looks at commercial practices involving the use or supply of electronic agents and the extent to which these could be deemed unfair in terms of the recent proposal for a Directive on unfair commercial practices.

1. Introduction

In the last few years, there has been an increased interest in electronic agents not just in fields such as computer science, philosophy and the social sciences but also in law. There is growing legal discourse on the legal issues and challenges arising from the use and operation of electronic agents in the electronic marketplace.[2]

---

[1] This article first appeared in R. Nielsen, S. Sandfeld Jacobsen & J. Trzaskowski (eds), *EU Electronic Commerce Law*, Djøf Publishing, Copenhagen, 2004, pp. 209-221.

[2] To mention but a few examples, projects funded by the European Commission such as ECLIP II (Electronic Commerce Legal Issues Platform – IST-1999-12278), ALIVE (Advanced Legal Issues in Virtual Enterprises – IST-2000-25459) and ALFEBIITE (A Logical Framework for Ethical Behaviour between Infohabitants in the Information Trading Economy of the Universal Information Ecosystem, IST-1999-10298) have focused on selected legal issues related to electronic agents, and conference workshops such as those on The Law and Electronic Agents (LEA 2002 and LEA 2003 - http://www.cirfid.unibo.it/~agsw/lea02/index.html, http://www.cirfid.unibo.it/~agsw/lea03/ (last visited 5.1.2004)) have also discussed a broad range of legal issues.

This paper will focus on autonomous, mobile software agents. Autonomy is an important characteristic of electronic agents and, in effect, means that such electronic agents operate without the direct intervention of human beings and have some kind of control over their actions and internal states.[3] Agents may also be mobile, in the sense that they can move to and from different locations on the Internet. They can communicate with other agents and interact with their environment.

Electronic agents may have a variety of functions. There are, for example, *search agents* which look for and gather information for their users, *filtering agents* which sift through the incredible amount of information available on the Internet and *broker agents* that mediate between online sellers and buyers. Electronic agents may possess a combination of these and other functions.

The scenarios examined in this paper deal with electronic agents that gather or obtain data (which may include personal data) from other electronic agents or from another person's computer system. The paper will not seek to examine further the reason for such actions, for example, in order to spread a virus or to commit fraud, blackmail or another crime, as these acts are typically already addressed and proscribed by many national computer misuse legislation.

The aim of this paper is not to paint a scenario of doom and gloom but to highlight some of the threats that may arise because of the increased use of intelligent agent technology, and to focus on some recent legislative responses in Europe to such threats.[4] Specifically, this paper will look at recent legislative developments in three areas: privacy and data protection, cybercrime and unfair competition.

2. Privacy

One of the main threats of electronic agents today is to personal privacy.[5] Agents can visit websites, select and collect certain data on individuals and deposit such data in databases. Where the collection is done in such a way as to enable the identification of individuals ("data subjects"), then such data

---

3 M.J. Wooldridge & N.R Jennings, "Intelligent Agents: Theory and Practice", Knowledge Engineering Review, Vol 10, No. 2, June 1995, pp. 115-152, Cambridge University Press, 1996.

4 Put more precisely, as regards privacy and data protection and unfair competition, the paper will look at recent developments in the European Union; whereas with regards to cybercrime reference will be made to an international instrument.

5 For an extended discussion of threats to privacy by electronic agents under the Data Protection Directive, see L.A. Bygrave, "Electronic Agents and Privacy: A Cyberspace Odyssey", 2001, *IJILT*, Vol.9, No. 3, pp. 275-294.

would be deemed to be personal data in terms of most current data protection legislation, not least of which the European Union's ("EU") Data Protection Directive, triggering the application of such legislation.[6] A profile may be built from keeping track of an individual's behaviour and used by companies to target certain products or services to that individual. Where, as is likely to be often the case, the surveillance is covert, fears of the development of an Orwellian society abound.

2.1 Agent surveillance

As mentioned above, agents may be mobile and may communicate with agents of other users and interact with their environment. It is possible that an electronic agent enters the terminal of a user without the knowledge of the user in order to gain access to information stored there. The Directive on privacy and electronic communications[7] acknowledges in its recitals that:

> *"so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users".*[8]

An electronic agent would fall within the general term "other similar devices". The use of such devices

> *"to store information or to gain access to information stored in the terminal equipment of a … user is only allowed on condition that the … user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC [the Data Protection Directive],* inter

---

6 The Data Protection Directive defines personal data as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". See Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995, pp. 0031-0050.

7 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/7/2002, pp. 0037-0047.

8 Recital 24, Directive on privacy and electronic communications, *op. cit.* fn. 7.

> alia *about the purposes of the processing, and is offered the right to refuse such processing by the data controller."*[9]

Thus, any covert intrusion by electronic agents whereby they gain access to information stored on the terminal equipment of the user either by directly accessing the terminal of the user or by interacting with spyware or other similar hidden devices on the user's terminal is prohibited.

Electronic agents may, thus, interact with cookies or with spyware residing in an individual's hardware. Spyware is software that has a tracking facility residing surreptitiously in an individual's computer, keeping tabs on the online activity of that individual and transmitting such data to the software provider. Such spyware may either be published as "freeware", "adware"[10] or packaged with a licensed software but, obviously, without the user being aware of its existence. Needless to say, the use of such electronic agents that interact with spyware or hidden identifiers without the knowledge of the user would be in breach of Article 5(3) of the Directive on privacy and electronic communications as discussed above. However, the Directive empowers Member States to allow the use of such covert devices where this

> *"constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".*[11]

It is perhaps worth pointing out that the Directive proscribes the act of gaining access to stored information on the user's terminal: it is thus irrelevant and not necessary, for this provision to come into effect, to also prove that such information has also been copied, transmitted or stored elsewhere, for example, in the data controller's network.

This Directive cross-refers to and applies the information duties that data controllers have towards data subjects under the Data Protection Directive, i.e. Articles 10 and 11. The data subject must therefore, besides details of the

---

9 Article 5(3), Directive on privacy and electronic communications, *op. cit.* fn. 7.

10 Adware is typically freeware which has advertisements embedded in the programme and which show up when the user opens the programme. Most adware authors provide the free version with ads and a registered version whereby the ads are disabled. Thus, it is the user who decides whether to use the freeware with ads or to licence a registered version. See further on this, *Spyware* at http://simplythebest.net/info/spyware.html (last visited 16.12.2003).

11 Article 15(1), Directive on privacy and electronic communications, *op. cit.* fn. 7.

purposes for the processing, also be provided with other information, such as the identity of the controller and any representative of his/her, the recipients or categories of recipients of the data, and the existence of the data subject's right to access and to have rectified the data concerning him/her.

As abovementioned, the user must also be provided with the right to refuse such processing. Thus, what the Directive requires is not that the user consents[12] to the processing of his/her data, but that the user does not refuse such processing.

The *raison d'être* of this provision is a recognition that the terminal equipment of users of electronic communication networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. The Directive on privacy and electronic communications applies to users who are natural persons using a publicly available electronic communications service for private or business purposes, without necessarily having subscibed to that service.[13]

The Directive recognised that devices such as cookies can be a legitimate and useful tool and the recitals cite as examples the use of cookies to analyse the effectiveness of website design and advertising and in verifying the identity of users engaged in online transactions. In such cases, the use of a device such as a cookie is allowed provided that the two conditions mentioned earlier in this paper are complied with: that the user (i) is provided with clear and precise information in accordance with the Data Protection Directive, and (ii) is given the option to refuse to have a cookie stored on his/her equipment.[14]

2.2 Surveillance or interception of communication of data

It should also be mentioned that the surveillence or interception of communications and the related traffic data by electronic agents would fall within the prohibition in Article 5(1) of the Directive on privacy and electronic communications. This Article exhorts EU Member States to "prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users without the consent of the users concerned, except when legally authorised to do so" to

---

12 In the Directive on privacy and electronic communications, "consent" has the same meaning as that found in Article 2(h) of the Data Protection Directive, i.e. "'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". See Article 2(f), Directive on privacy and electronic communications, *op. cit.* fn. 7.

13 In fact, this is the definition of "user" in Article 2 (a) of the Directive on privacy and electronic communications, *op. cit.* fn. 7.

14 See Recital 25, Directive on privacy and electronic communications, *op. cit.* fn. 7.

safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. Thus, collecting click-through data and other web browsing information can constitute a violation of this provision where this is without the consent of the user. However, any legally authorised recording of communications and related traffic data carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication is allowed.[15]

3. Cybercrime

The scenarios described in this paper such as obtaining access to data and surveillance may also be proscribed under the Convention on Cybercrime,[16] when this Convention enters into force and is implemented into the law of the states which ratified it.[17] Two articles of this Convention are of particular relevance in this context – Article 2 on illegal access and Article 3 on illegal interception.

3.1 Illegal access

The access to the whole or any part of a computer system without right and when committed intentionally is proscribed by the first part of Article 2. Two questions may immediately be raised. What constitutes "without right" in this context, and how is intentionality to be understood when the access is sought and obtained by an intelligent agent acting autonomously, i.e. without the knowledge or direction by the person who activated the agent?

3.1.1 Access without right

Where the owner or other rightholder of the computer system or part of it has authorised access (e.g. to test the security of the system), this is not an infringement of Article 2. The Explanatory Report to the Convention also provides that there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right".[18]

---

15 Article 5(2), Directive on privacy and electronic communications, *op. cit.* fn. 7.

16 Convention on Cybercrime, signed at Budapest, 23.11.2001, Council of Europe ETS No. 185.

17 To date, the Convention on Cybercrime has not yet entered into force. By end December 2003, it has been ratified by Albania, Croatia, Estonia and Hungary. It requires ratification by one other state to enter into force.

18 Explanatory Report to the Convention on Cybercrime, para. 47.

Sometimes, the application of certain technical tools such as cookies or bots to locate and retrieve information may result in an access under Article 2. The Explanatory Report provides that the application of such devices is not *per se* "without right":

> *"The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself "without right", in particular where the rightholder of the accessed system can be considered to have accepted its application, e.g. in the case of "cookies" by not rejecting the initial instalment or not removing it."*[19]

This illustrates the broad scope of the abovementioned first sentence of Article 2. The drafters of the Convention recognised this and allowed Parties to the Convention to take a narrower approach by attaching certain qualifying elements to the access proscribed in the first sentence of Article 2. In fact, Article 2 further provides that a state implementing this provision

> *"may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."*

Thus, where an Internet user deploys an electronic agent to breach another user's security measures such as a firewall, or by using an illegally obtained password, the access would be illegal in terms of Article 2.

The access must be of "the whole or any part of a computer system". What happens if the electronic agent of company X obtained data from the electronic agent of user Y? Is the electronic agent of Y to be deemed as "part of [the] computer system" of Y? The term "computer system" is defined as:

> *"any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".*

Furthermore, the Explanatory Report explains that:

> *"A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output and storage facilities. It may stand alone or be connected in a network with other similar devices. …"*[20]

---

19 Explanatory Report to the Convention on Cybercrime, para. 48.

20 Explanatory Report to the Convention on Cybercrime, para. 23.

Let us illustrate the above example further. Imagine the electronic agent of Y was a software agent licensed by Y and intitated by him from his computer system to identify, select and buy a weekly cinema ticket for Y. The agent interacts with other software in Y's computer system (e.g. a data file which contains Y's bank details, Y's calendar or personal digital assistent). It is submitted that such a software agent should be deemed to be part of the computer system of Y. However, what if the data was intercepted while the electronic agent – a mobile agent - of Y had migrated to another platform to search for the best priced ticket? Doubts could be raised whether the agent could still be deemed to be part of Y's computer system and hence, whether Article 2 would be applicable. It is submitted that, in any case, such behaviour would fall within Article 3 of the Convention, dealing with unlawful interception of data.[21]

3.1.2 The question of intention

Though one might be able to prove the existence of the material elements (*actus reus*) of the offence in the first sentence of Article 2, that is:

i) the access to the whole or part of a computer system
ii) without right,

for the offence to subsist, one must also prove the existence of the intentional element (*mens rea*), i.e. that the access is "committed intentionally".

The difficulty that might arise is how the prosecution in a criminal case – where the standard of evidence required in most countries is proof beyond reasonable doubt[22] - may ascribe the actions of an autonomous intelligent agent to the person who initiated it (the user). It is submitted that this is a question of fact and depends on the circumstances of each particular case. It would depend on factors, for example, such as: whether the user had himself designed and written the software agent, whether the user had initiated the agent (i.e. supplied it with its terms of reference – what it should or perhaps even should not do), the type of electronic agent software deployed to carry out a particular task and its suitability thereto (e.g the reputation of such types of software agents), etc. In other words, as often happens in criminal matters, the actions or omissions of the user very often reflect and can be used to infer his/her state of mind (intention).

---

21 See section 0 below.

22 This is in contrast to the standard often required in civil suits which usually requires a balance of probabilities.

3.2 Unlawful interception of data

Article 3 of the Convention outlaws:

> *"when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data."*

It is clear from the Explanatory Report that the term "technical means" includes "the use of software" and hence, it is submitted, also interception by software agents.[23] The requirement of using technical means was meant by the drafters as a restrictive qualification to avoid over-criminalisation.

3.3 The importance of a causal link with the user: the "Trojan horse" defence

Electronic agents can operate as a kind of "Trojan horse" on another person's computer system. A mobile agent can move to another person's computer and carry out certain operations from that computer, without the knowledge or consent of that computer's user or owner, an act that is likely to be proscribed by most national laws on hacking and by Article 2 of the Convention on Cybercrime. In the UK, the "Trojan" defence – that one's computer has been taken over for the commission of a crime by someone else who has hacked into the computer - has been successfully used in two cases where the owner of a computer was charged with a computer crime (respectively, hacking into another computer system and possession of child porn).

What was of particular interest in the former of these cases,[24] dealing with a severe denial-of-service attack on the port of Houston in Texas, is that this defence was successful even though prosecution experts could find no evi-

---

[23] Explanatory Report to the Convention on Cybercrime, para. 53.

[24] Mr. Aaron Caffrey was accused of crashing systems at the port of Houston in Texas by hacking into its computer system, and faced one charge at Southwark Crown Court in the UK of unauthorised modification of computer material. The port's computer system was bombarded with thousands of electronic messages, freezing its web service which contained vital data for shipping, mooring companies and support firms responsible for helping ships navigate in and out of harbour. Mr Caffrey admitted being a member of a group called Allied Haxor Elite and hacking into computers for friends to test their security, but he insisted he was not responsible for the attack on the port of Houston. Both the defence and prosecution acknowledged that the attack came from his computer. The jury believed the defendant's argument that his computer had been taken over by a hacker using a Trojan horse program. A forensic examination of Mr Caffrey's computer had found no trace of a hidden program with the instructions for the attack. See further on this "Questions cloud cyber crime cases", BBC News, 17 October 2003, http://www.bbc.co.uk/go/pr/fr/-/2/hi/technology/3202116.stm (last visited 15.12.2003).

dence that the accused's computer had been broken into. Moreover, both the defence and prosecution acknowledged that the attack came from the defendant's computer. The danger, as Dave Morrell, a computer consultant for the Houston pilots who worked with the FBI after the attack, explained, is that this defence "sets a precedent now in the [English] judicial system where a hacker can just claim somebody took over his computer, the program vanished, and he's free and clear".[25] It is perhaps not inconceivable that a similar defence would be attempted by the owner of a deviant electronic agent whose acts could amount to a criminal offence, i.e. that the agent was hijacked by another agent. In today's complex computer network architecture, it may be difficult to prove a causal connection between an electronic agent which has acted deviantly and the person (including such person's electronic agent) who controls or took over control of the agent. However, the danger of using a defence such as the "Trojan horse" defence in situations where there is no evidence that a computer system or part of it has been taken over by a hacker, can considerably water down the effectiveness of criminal sanctions such as those in the Convention on Cybercrime discussed above.

4. Unfair commercial practices

4.1 Aggressive commercial practices

Among the abilities of intelligent agents is that of targeting a service or a product that fits the specific needs of a customer at the opportune time, i.e. when the customer is likely to need such service/product. Such agents can be a very effective marketing and sales help to the seller, and also of assistance to prospective buyers in identifying the right product and the right seller or service provider for their needs. There have, for example, been cases in some countries where parents of newly born babies have been sent samples of baby food or brochures of baby-related products such as prams, nappies, etc. Such type of behaviour by companies is usually considered acceptable as long as it is reasonable and not abusive. The proposed Unfair Commercial Practices Directive[26] prohibits what it calls "aggressive commercial practices", that is a commercial practice:

---

[25] E. Mills Abreu, "Hackers get novel defense: The computer did it", *Computerworld*, 28 October 2003, http://www.computerworld.com/printthis/2003/0,4814,86600,00.html (last visited 16.12.2003).

[26] Proposal for a Directive of the European Parliament and of the Council concerning unfair business-to-consumer practices in the Internal Market and amending directives

> *"where by harassment, coercion or undue influence, it significantly impairs or is likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise."*

"Undue influence" is further defined in the Proposal as:

> *"exploiting a position of power to apply pressure, without using physical force, in a way which significantly limits the consumer's ability to make an informed decision."*

Among the factors to be used to determine whether a commercial practice uses harassement, coercion or undue influence are *inter alia* its timing, nature or persistence,[27] the use of threatening or abusive language or behaviour,[28] and the use by the trader of any specific misfortune or circumstance of such gravity as to impair the consumer's judgment, of which the trader is aware, to influence the consumer's decision with regard to the product.[29] For example, the targeting of consumers who have recently suffered a bereavement or serious illness in their family in order to sell a product which bears a direct relationship with the misfortune is considered by the Proposal to be an aggressive commercial practice and hence outlawed.[30] The Proposal, in an Annex, contains a blacklist of commercial practices which are considered in all circumstances to be unfair.

The aim of the Proposal is to strike a balance between business needs (e.g. to increase profit, to expand) and the protection of consumers (e.g. protection from exploitation, from making a decision he/she would not have otherwise made).

4.2 Unfair practices

Commercial search agents are often used by consumers to help them search for, identify and purchase goods or products from online retailers. It is not inconceivable that a search agent of this kind would have a bias towards

---

84/450/EEC, 97/7/EC and 98/27/EC (the Unfair Commercial Practices Directive), 18.6.2003, COM (2003) 356 final.

27 Article 9(a), Proposal for an Unfair Commercial Practices Directive, op. cit. n. 26.

28 Article 9(b), Proposal for an Unfair Commercial Practices Directive, op. cit. n. 26.

29 Article 9(c), Proposal for an Unfair Commercial Practices Directive, op. cit. n. 26.

30 Annex 1, paragraph (4) of the list of aggressive commercial practices, Proposal for an Unfair Commercial Practices Directive, op. cit. n. 26.

certain websites. Though such a search agent may operate autonomously, i.e. without the direct intervention or control of a human being, it does not mean that behind the scenes, there could not be an agreement(s) between some companies advertising their products or services on the Internet and the company controlling the search agent's functions. It has, until now, not been clear whether such "defects of neutrality" are proscribed at an EU level since there is no Community legislation on unfair competition in force as yet.[31] The question arises whether this would be proscribed by the recent proposal for a Directive on unfair commercial practices, if and when this Directive is passed. It should be mentioned that the proposal applies only to business-to-consumer transactions and not to business-to-business transactions.

The proposed Directive defines the conditions which determine whether a commercial practice is *un*fair. It does not impose any positive obligations which a trader has to comply with to show he is trading fairly. The proposal contains a general prohibition of unfair commercial practices and also provides two key types of unfair commercial practices – those which are misleading and those which are aggressive. Misleading commercial practices can be either misleading actions or misleading omissions.

The general prohibition of unfair commercial practices establishes three conditions for determining whether a practice is unfair, all three of which have to be proven in order for the practice to be judged unfair:[32]

- the practice must be contrary to the requirements of professional diligence
- the practice must materially distort or be likely to materially distort the consumer's economic behaviour
- the benchmark consumer to be considered is the "average consumer", i.e. a consumer who is reasonably well informed and reasonably observant and circumspect.

It is submitted that the provision of a biased software agent by a trader is not, *per se*, enough to constitute an unfair commercial practice. The consumer might, for example, reasonably expect a search agent provided on a particular website to have a certain bias towards the products or services of the group of companies of which that website company is known to form part. Such a practice cannot be said to be "contrary to the requirements of professional diligence" which is defined in Article 2 (j) as "the measure of

---

31 For further discussion of this, see S. Feliu, "Intelligent agents and consumer protection", IJILT, Vol. 9, No. 3, 235-248, in particular at pp. 243-244.

32 Article 5(2), Proposal for an Unfair Commercial Practices Directive, op. cit. n. 26. See also the explanatory memorandum to the proposal, para. 51.

special skill and care exercised by a trader commensurate with the requirements of normal market practice towards consumers in his field of activity in the internal market". However, if the search agent is touted as a neutral agent by the website owner, when in fact it is not, then this could be deemed to be against the requirements of professional diligence.

It is also submitted that the licensing of a search agent software acquired by a consumer principally for its search functions/qualities but which, in fact, does not have neutral search functions, is likely to be deemed to be a misleading omission in terms of Article 7 of the Proposed Directive which considers misleading a commercial practice:

> *"which, in its factual context, taking account of all its features and circumstances, omits material information that the average consumer needs, according to the context, to take an informed transactional decision and thereby causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise."*[33]

Article 7(2) also regards as a misleading omission the situation

> *"when a trader hides or provides in an unclear, unintelligible, ambiguous or untimely manner such material information or fails to identify the commercial intent of the commercial practice."*

A transactional decision includes a decision about whether to buy and from which supplier.[34] In this specific example, it is reasonable to assume that the consumer would not have licensed that particular software agent had he/she known that that electronic agent had a defect of neutrality.

What about the provision of a software agent which contains spyware that sends information about customers to the seller who provided the agent? Besides being in breach of the Directive on privacy and electronic communications as explained above,[35] it is submitted that this would also be considered a misleading action and, hence, an unfair practice by the proposed Directive on unfair commercial practices. Article 6 prohibits a commercial practice that "causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise because it deceives or is likely to deceive him in relation to the main characteristics of the product, such as its … risks, … composition, accessories, … or the results

---

33 Article 7(1), Unfair Commercial Practices Directive, op. cit. n. 26.

34 Explanatory Memorandum to the Proposal for an Unfair Commercial Practices Directive, para. 55.

35 See section 0 above.

to be expected from its use." Had the consumer been aware of the existence of the hidden spying features in the software agent, he/she might not have acquired or accepted such software in the first place.

The Proposal is thus a step in the right direction in that it addresses a number of threats to consumer transactions, including those made online and which may involve the use of electronic agents. It now remains to be seen whether and, to what extent, the proposed Directive on unfair commercial practices is adopted.

5. Concluding remarks

Autonomous software agents have often been hailed as revolutionary tools, assistants or helpers for actors in the electronic marketplace such as buyers, sellers and service providers. In this paper, an attempt has been made to highlight some of the threats arising from the use of such agents and to discuss some recent developments in Europe in three fields of law, viz. privacy and data protection, cybercrime and unfair competition. As discussed in this paper, these recently enacted or proposed pieces of legislation address many of the threats arising from the use of agents in the electronic marketplace. However, the indiscriminate use of certain defences, such as the "Trojan horse" defence in situations where no evidence of hacking is found, can water down the effect of such laws. Moreover, one should also recognise that the state-of-the-art of agent technology and the marketplaces in which such agents operate is still in its infancy and it is likely that more challenging legal questions will be raised when more sophisticated autonomous agents are available.

6 REPUTATION SYSTEMS AND DATA PROTECTION LAW[1]

By Tobias Mahler & Thomas Olsen

Abstract: Reputation systems can be used to provide relevant information about others when we interact with persons we do not know. However, reputation systems are challenged by concerns about privacy and data quality. This paper assesses how data protection law affects the design and the operation of reputation systems.

1. Introduction

Reputation systems collect information about a person or other entity (hereinafter "reputation subject") in order to evaluate the reputation subject's conduct and make this evaluation accessible for other users' decisions. An example is when Internet marketplaces like eBay* and Amazon.com* enable users to provide feedback on other users. In this case, feedback ratings are based on a user's past transactions and help other users learn about the transaction partner they are dealing with. Other examples include credit reporting services, which collect information about an entity's economic behaviour. This information is communicated e.g. to banks when they decide about credit. The latter kind of reputation systems has existed for a long time, but recent developments with respect to Internet based transactions have led to an increased need for reputation systems for this context.

Reputation systems may be of particular value when there is uncertainty about another person or entity involved in a planned transaction that involves risk. Transactions on the Internet involve a number of uncertainties with regard to the identity of the transaction partner, his or her ability and

---

[1] This paper was originally prepared for the eChallenges conference, Vienna 27-29 October 2004, and is published in the proceedings of the conference and in the book P. Cunningham & M. Cunningham (eds.), eAdoption and the Knowledge Economy: Issues, Applications, Case Studies, part 1, ISBN 1 58603 470 7, IOS Press, Amsterdam 2004, pp. 180-187. The research work has been partly financed by the European Commission through the project TrustCoM (A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations) and partly financed by the Norwegian Research Council through the project Personalised Internet-Based Services and Privacy Protection – PerProt.

willingness to perform and the availability of realistic means of enforcement. The lack of experiences, knowledge or information about the other person or entity may lead us to refrain from the interaction. Reputation systems can provide us with relevant experiences others have had with this person or entity. Research indicates that reputation systems can encourage market actors to participate in transactions [i]. Reputation systems have also been considered as a compensation or supplement for lacking realistic means of enforcement on the Internet [ii, iii, iv]. Thus, it is possible to think of new application scenarios for reputation systems, e.g. within virtual communities. The possibilities offered by reputation systems are promising, but one should also pay attention to possible threats.

2. Objectives and Methodology

The objectives of this paper are to investigate privacy and data protection problems related to reputation services. Introducing a reputation system requires a rather extensive collection, evaluation and disclosure of data. When deciding whether or not to participate in a reputation system, a potential user's concern may be whether the system will meet reasonable expectations with respect to privacy. Users may fear that too much information about them is collected and disseminated. There may also be concerns with regard to the "judging function" of a reputation system, where a user's conduct is evaluated. Such evaluations may be significant, since they are meant to be the basis for future decisions concerning him or her. This may raise questions with regard to how the user can dispute an evaluation he or she disagrees with. The lack of transparency and comprehensibility may increase these concerns. All these privacy-related concerns and fears may weaken the acceptance of a reputation system by potential participants.

Privacy concerns are not the only factors that can mitigate the uptake of a reputation system. From the perspective of the entity that uses the reputation profiles for decisions, the relevance and accuracy of the reputation data is essential. This decision-maker is interested in optimized data quality and has a separate interest in the quality of the process that generates reputation profiles. If the quality is not satisfying from this perspective, this may weaken the value and utilization of the reputation system.

Data protection law provides rules that secure a fair processing of personal data. Furthermore, data protection law aims at enhancing data quality and contributes to increased transparency with respect to how data is processed. Therefore, data protection law can contribute to improve the value, acceptance and uptake of reputation systems.

The aim of this paper is to provide guidelines for the design of reputation systems from a data protection perspective. It identifies legal and technical issues that should be addressed in order to design lawful and legitimate reputation systems. We will not analyse a specific reputation system, but rather explore different possibilities when developing a reputation system. Technical and organisational design choices may have legal consequences, particularly with respect to data protection law.

3. Data Protection Law

In Europe, data protection is subject to a rather strict legislation both on the European and national level. In this respect, reference will be made to the EC Directive on Data Protection (hereinafter EC Directive [v]) and its implementations in relevant national acts on privacy and data protection. A reputation service dealing with personal data is bound to follow the applicable national data protection law.

3.1 Who is Who in Data Protection Law

This section will introduce the central actors and terms used in this paper to analyse reputation systems in the light of data protection law.

Personal data: This term is defined in the EC Directive, Article 2, as "any information relating to an identified or identifiable natural person". "Any information" is a rather wide wording, which includes everything that can be perceived, sensed or registered etc. about a person. There are reasonable arguments to hold that also opinions, even false ones, must be qualified as personal data [vi]. An "identifiable person" is one who can be identified, "directly or indirectly". Some of the data processed by reputation systems can be personal data. However, the data will only fall into this category, if the data subject is a "natural person".

Data subject: In data protection law, the data subject is the natural person (individual) to whom the personal data refers. However, reputation systems may also hold data that refers to other entities than individuals. We will therefore introduce the term "reputation subject".

Reputation subject: A reputation system can in principle administrate the reputation of individuals, groups, organisations, collective entities (may be legal persons). This paper does not deal with objects in reputation systems. We will use the term reputation subject when referring to the entity to which the reputation data relates. In principle, reputation systems must only comply with data protection law when processing data on individuals. Other entities protection is usually limited to laws dealing with defamation, breach of con-

fidentiality and unfair competition. This is in contrast to data protection law, which e.g. ensures data quality, i.e. that data are relevant, correct, complete and not misleading in relation to the purposes for which they are processed. Arguably, collective entities and individuals share some interests, particularly with respect to the quality of data [vii]. Therefore, reputation system providers may want to choose to follow central data protection rules also when processing data on other reputation subjects.

Data controller: In the EC Directive, the data controller is defined as anybody who determines the purposes and means of the processing of personal data. When deciding who is a data controller in a reputation system, one has to identify the person or organisation with decision making power. If the system is developed by one entity but independently used by another, the latter is the data controller, since this entity determines the purposes and means of the processing. In principle, it is not impossible to think of more than one data controller. Data controllers are responsible for the lawful processing and may be held liable.

3.2 Basic Principles

The most important rules in data protection law can be expressed in relation to a number of basic principles [viii] to be found in most international and national data protection instruments and laws.

Fair and lawful processing: Personal data must be processed fairly and lawfully.
Purpose specification: Personal data must be collected for specified, explicit and legitimate purposes and not further processed for other purposes.
"Minimality": The collection and storage of personal data should be limited to the amount necessary to achieve the purpose(s).
Information quality: Personal data should be valid with respect to what they are intended to describe and relevant and complete with respect to the specified purpose(s).
Data subject participation and control: Persons should be able to participate in the processing of data on them and they should have some measure of influence over the processing.
Limitation of fully automated decisions: Fully automated assessments of a person's character should not form the sole basis of a decision that impinges upon the person's interest.
Disclosure limitation: The data controllers' disclosure of personal data to third parties shall be restricted, it may only occur upon certain conditions.
Information security: The data controller must ensure that personal data is not subject to unauthorised access, alteration, destruction or disclosure.

Sensitivity: Processing certain categories of especially sensitive data is subject to a stricter control than other personal data.

4. Data Protection Law and Reputation Systems

In this section, we will correlate these principles of data protection law with some of the possible characteristics of reputation systems. When designing a reputation system, one is confronted with a number of technical and organisational choices. These choices have an impact on how the reputation system processes personal data.

4.1 Participation in Reputation Systems

The principle of fair and lawful processing generally requires data controllers to take account of the interests and reasonable expectations of data subjects. This also implies that data subjects should not be unduly pressured into participation in reputation schemes. The principle of fair and lawful processing is embodied in a number of requirements in data protection law. The data subject's consent is the most important criterion to make processing of personal information in reputation systems lawful. The EC Directive defines the data subject's consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Articles 2 (h) and 7). The Directive requires timely and comprehensible information to be provided to the data subject, and the consent should be expressed through a freely and positive action. One should note that the processing of personal data also may be lawful without consent if other criteria are fulfilled. This may be the case, e.g. if the data controller's interest overrides the privacy interest of the data subject, or if the processing is necessary in relation to a contract or a legal obligation (Article 7(b), (c) and (f)).

When implementing a reputation system, one may consider making it mandatory to achieve maximum participation and value of the system. Most auction sites have a mandatory reputation system where participation in the reputation system is a condition for using the services. A discretionary/optional reputation system might be an alternative to be considered, even though this may cause some practical disadvantages.

4.2 Centralised and Distributed Reputation Systems

The current reputation systems that have seen some form of deployment are centralised in the meaning that there is one centralised reputation service

provider. For example in Amazon.com, information is centrally administrated.

This can be compared to distributed reputation systems, where every entity runs a local instance of the reputation system. Also hybrid systems have been suggested, combining elements characteristic for centralised and distributed reputation systems [ix]. One advantage with a distributed reputation system from a data protection perspective could be that information is spread between all participants, thus hindering accumulation of information in one place. Even in a fully distributed system, the system designer should ensure that relevant data protection principles are respected, including the right to access own personal data and the possibility to rectify false sets of data. In some cases it may be difficult to identify the data controller(s) in distributed systems.

Obreiter has suggested the use of so-called "evidences" in distributed reputation systems [x]. These non-repudiable tokens describe the behaviour of a specific entity in a statement. Digital signatures are used to make sure that the statement can be passed on to others. For example one party in a transaction can pass an evidence token to the other party, declaring the receipt of the item they trade. This receipt can later be used in order to document the behaviour, i.e. that the item has been sent and was received. In a data protection perspective, the use of such tokens has the advantage that they are not controlled by a central instance, but by the data subject himself. However, if the statements are too detailed and the data subject is expected to transfer many such tokens in order to document trustworthiness, this could lead to an excessive dissemination of personal information.

4.3 Identity and Identification

Reputation subjects may participate in a reputation system disclosing their real life identity to the other participants, or they may act under a pseudonym. From a data protection point of view, this choice is one of the most fundamental issues. One has to consider the necessary functionality of the reputation system and should be aware of technical, organisational and legal means to protect the identities and the personal data of the users.

"Personal data" is defined in the EC Directive, Article 2, as "any information relating to an identified or identifiable natural person". An "identifiable person" is one who can be identified, "directly or indirectly" within a reasonable time, considering the necessary effort taking account of all the means likely reasonably to be used. Existing reputation systems often use pseudonyms to hide the identities of the users. We are not aware of fully anonymous reputation systems. In eBay for example, users register their contact information and are provided with a pseudonym which is used for transactions on

the marketplace. Since the person behind the pseudonym can be identified, the pseudonym itself and data related to the pseudonym are personal data in relation to the EC Directive. It is possible to think of "strong" or "weak" pseudonyms in relation to how difficult it is to reveal the real-world identity for other users of the reputation system [xi].The disclosure limitation principle provides that strong pseudonyms should be preferred to weaker ones.

When issuing a pseudonym, the reputation system has different possibilities to verify the identity of the person. If a strict verification procedure is implemented, this strengthens the possibilities of holding the user of a pseudonym liable for misconduct. Pseudonyms that are linked to a verified identity may be trusted more easily. It is also possible to think of reputation systems where parties could participate under different pseudonyms depending on the need for assurance and reliability [xii]. If a reputation system allows the use of multiple pseudonyms, these should not be linked to one common reputation profile [xiii].

Reputation systems should be limited to a specific marketplace or environment. A general reputation service that covers all kinds of actions in different contexts may lead to an excessive disclosure of personal information. Therefore, one should be careful with linking profiles from different reputation systems.

4.4 Types of Data in Reputation Profiles

A reputation system can generate a reputation profile by combining elements of evaluation ("excellent eBay buyer") with more factual elements regarding e.g. the timeliness of the transaction, its value or category. In this context, fact and evaluation are not seen as two dichotomist categories. This is rather a question of degree. For example, the comment "timely delivery" may include elements of both facts (delivery date) and evaluation (relation of the delivery date to rules about delivery, e.g. in a contract).

Some reputation systems, e.g. within credit rating, are based fully or mainly on factual information. Facts can either be made available to the end-user as separate information in order to provide a more comprehensive picture of the reputation subject, or they can be combined with the evaluation. The reputation system can collect factual information from a party's declaration, or simply track some of the information that is processed in relation to a transaction. Any collection from the data subject must be done in a fair and lawful way. This may require an informed consent, i.e. the participant must fully understand what is being tracked and for what purposes the data will be used. Ideally this should be explained both in a detailed way and in a way that is understandable for the average participant. This must be done *prior* to the collection of information.

The other element in reputation systems consists of evaluations, normally provided by other participants. In a data protection context, this is classified as the collection of personal data from third parties. The reputation system must additionally ensure that the data subject is informed about the fact that personal data is collected from others. Evaluations may be thought of as rather uncomforting by the reputation subject, since this can be perceived as a judgment about him or her. Two data protection principles can assist the reputation subject in such situations: The principle of data quality and the principle of the data subject's participation and control. Both principles are reflected in Art. 12 (b) of the EC Directive, according to which the data subject has a right to have incomplete or inaccurate data rectified, erased or blocked. Obviously, evaluations made by third parties are difficult to verify for reputation systems. To cope with this problem, some reputation systems allow participants to cross-comment evaluations. Interestingly, research has shown that this function in eBay's feedback system leads to an under-reporting of negative comments because of the fear for negative cross-comments [xiv]. However, while minor problems are under-reported, participants do report instances of fraud, which indicates that the system seems to work best when it is most needed [xv].

4.5 Generation of Reputation Profiles

Reputation profiles can be generated by aggregating factual elements and evaluations. This can result in some kind of score, e.g. a number of stars (Amazon.com) to be communicated to other users. According to the EC Directive, Article 12 (a), the data subject has a right to access the "knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions". Automatic decisions based on reputation profiles will be discussed below in section 0. However, we can already state that this may require that reputation systems have to inform the data subjects about the algorithm that is used to generate the reputation profile. Additionally, the algorithm has to comply with the principle of information quality in the sense that it generates information that is relevant, adequate and not excessive in relation to the purpose of the processing.

4.6 Access to and Disclosure of Reputation Data

Any data subject has a general access right to data on himself or herself (Art. 12). In the sequel, we will explore the limitations with respect to the disclosure of data to third parties.

Access to reputation data by third parties must be dealt with in light of the disclosure limitation principle. According to this principle, the data controller's disclosure of personal data to third parties shall be restricted, it may

only occur upon certain conditions. The data subject may consent to such disclosure. Reputation data may be accessible all the time for any interested party, for example on a web site. Alternatively, access may only be given individually upon request.

When designing a reputation system, one should have in mind that some types of data are more sensitive than others. The EC Directive contains a catalogue of categories of especially sensitive data, which for example includes data concerning health or sex-life (Article 8.1.). This kind of data can only be processed under certain conditions. A reputation service that deals with data categories contained in this catalogue must restrict the disclosure to certain cases instead of allowing everybody to access the reputation data. Additionally, also other categories of personal data may have a strong impact or importance for a person, even though the category is not included in this catalogue. The sensitivity of personal data depends on its context. One example could be a person's credit history when applying for a credit. The importance of this type of data has led to special rules in some countries, even though financial information is not classified as sensitive.

In this respect, reference should be made to the rules about credit reports under Norwegian [xvi] and Swedish law [xvii]. These rules regulate the disclosure of credit information by professional actors who specialise on trading such data. For example, disclosure of credit information is only allowed if the requestor has a legitimate interest in receiving the data. Additionally, every time the recorded information about an individual is disclosed upon request, the credit information service has to contact this person (normally by letter). The data subject must be informed that data has been disclosed upon request, who has requested it and what has been communicated. Here, also legal persons are provided rights of access to information. This is one of the few examples where data protection law extends its scope to others than individuals.

The rules on credit reporting are the only set of rules that specifically regulates some reputation systems. However, it applies only to credit agencies. Other reputation services are not (yet) subject to specific regulation. Nevertheless, the main safeguards and procedures could be used analogously in other contexts where a reputation system deals with sensitive information. Reputation systems should consider following some of these procedures in order to ensure the acceptance of their system.

4.7 Decisions Based on Reputation Profiles

The major aim of reputation systems is to provide a basis for well-informed future decisions. In the cases of eBay and Amazon.com, the decision is whether or not to trust a certain pseudonym in the online market place. Decisions related to other reputation systems could include whether or not to

participate with a subject in a virtual organisation, whether or not to allow a member of a virtual community access to a certain resource, whether or not to avail a credit to a person etc. There are basically two ways how these decisions can be made. Either the decision maker decides freely and uses the registered reputation as one of the premises for a decision. Alternatively, the decision can be made automatically on the basis of the calculated reputation score. Automatic decisions are considered as problematic in a data protection perspective, and there are special rules for such decisions.

Article 15 limits the use of certain automatic decisions based solely on automatic processing of data [xviii]. This applies only to decisions that are legally binding or which significantly affect the data subject. The data processed must be intended to evaluate certain personal aspects of the person who is targeted by the decision. These personal aspects include performance at work, creditworthiness, reliability, conduct etc, which all are aspects that could be evaluated in a reputation system. As mentioned above in section 0, the data subject has a right to be informed about the logic involved in any automatic processing of data concerning him or her (Article 12 (a)). The data subject may also object to an automated decision and require a decision by a human (Article 15 (1), exceptions in (2)). Hence, when opening for automatic decisions based on reputation scores, one should be aware of these restrictions as implemented in national law.

5. Concluding Remarks

Reputation systems should be carefully designed in order to comply with data protection law, if they (at least in part) deal with personal data. This will ensure a fair administration of information and users will more easily accept to participate in the reputation system. The above mentioned basic data protection principles can also be considered as a means to improve the data quality in a reputation system, which makes the reputation system more relevant as a basis for a decision and more attractive for the end-user. Below, we have tried to capture some relevant factors that should be considered to ensure that reputation systems respect data protection law.

- Participation in a reputation system should be limited to actors who have expressed their well-informed consent.
- The purpose(s) of the reputation system should be clearly defined.
- The collection, storage and dissemination of (personal) data should be limited to the amount necessary to achieve the purpose(s).

- The procedures regarding the collection and evaluation of personal data should be transparent and communicated in a comprehensible way.
- Reputation subjects should be allowed some participation and control with respect to the collection of data about them and with regard to the generation of their reputation profile.
- The quality of both the collected data and of the aggregated reputation profile should be valid with respect to what they are intended to describe and relevant and not incomplete with respect to the specified purpose(s).
- Fully automated decisions on the basis of reputation profiles should be avoided. If they are chosen, there should be full transparency regarding the algorithms used to calculate the reputation score and to make the decision. Additionally, the data subject should be able to claim a human decision.
- The security of (personal) data must be ensured.
- Reputation systems that deal with sensitive data should use a stricter policy to protect personal data.

These recommendations may assist in identifying legal problems, indicating that the reputation system developer and the data controller should seek legal advice to clarify how the law in the relevant jurisdiction solves these issues. The recommendations may also be used as a point of departure for future research on reputation systems with regard to data protection law.

References

* Trademark or registered trademark of eBay Inc., Amazon.com Inc. and PEZ Candy Inc.

[i] Keser, C., Experimental games for the design of reputation management systems, IBM Systems Journal, Vol. 42, No. 3, 2003, pp. 498–506.

[ii] Friedman, D., Contracts in Cyberspace, available at http://www.daviddfriedman.com/Academic/contracts_in_%20cyberspace/contracts_in_cyberspace.htm, last visited 23 April 2004.

[iii] Gilette, C.P., Reputation and Intermediaries in Electronic Commerce, Louisiana Law Review, Summer 2002, pp. 1165–1197.

[iv] Block-Lieb, S., E-Reputation: Building Trust in Electronic Commerce, Louisiana Law Review, Summer 2002, pp. 1199–1219.

[v] Directive 95/46/EC, Official Journal L281, 23/11/1995 pp. 31–50.

[vi] Bygrave, L., Data Protection Law, Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague, London, New York, 2002, p. 46.

[vii] Bygrave, supra note vi, chapter 12.

[viii] Bygrave, supra note vi, pp. 57–68 and 2.

[ix] Fernandes, A. Kotsovinos, E., Östring, S. Dragovic, B., Pinocchio: Incentives for Honest Participation in Distributed Trust Management, in Trust Management, Second International Conference, iTrust 2004, LNCS 2295, pp. 63–77.

[x] Obreiter, P., A case for Evidence-Aware Distributed Reputation Systems, Trust Management, supra note ix, pp. 33–47, p. 39.

[xi] Clarke, R., Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice, http://www.anu.edu.au/people/Roger.Clarcke/DV/UIPP99EA.html, last visited 29 April 2004.

[xii] See for example the RAPID-project, Roadmap for Advanced Research in Privacy and Identity Management, http://www.ra-pid.org/, last visited 29 April 2004.

[xii] See also Seigneur, J.-M and Jensen, C. D., Trading Privacy for Trust, Trust Management, supra note ix, pp. 93–107.

[xiii] Gilette, supra note iii, p. 1191.

[xiv] Block-Lieb, S., supra note iv.

[xv] Norwegian regulation on the processing of personal data, Forskrift om behandling av personopplysninger (personopplysningsforskriften) section 4.

[xvi] Sweden's Credit-Reporting Act, Kreditupplysningslag (SFS 1973:1173).

[xvii] For more details about Art. 15 refer to Bygrave, L., Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling, Computer Law & Security Report, 2001, volume 17, pp. 17–24.

7 TELECOMMUNICATIONS AND THE REGULATORY REGIME IN NIGERIA.

By Peter Chukwuma Obutte

Abstract

A new law has been enacted in Nigeria for the regulation of the telecommunications sector[1].

This notwithstanding, as the wind of positive and startling dynamism continue to blow across nations in telecommunications sector, one important attraction it holds for developing nations can be traced to possibilities. That of an enduring and economic development, if properly nurtured and managed to reflect the National Telecommunications policy as now substantially represented in the legislation.

The straitened circumstances which however, characterise lives of a larger part of the nation's population no doubt require attention. The maximum realisation of these technological benefits however intensely desired by a country is largely tied to the existence of identifiable parameters as well as coherent principles for the telecommunications sector regulation sanctioned by the law and implemented in accordance with letters and intents of the law.

Since the country has scaled the first huddle by making the law, what about its implementation?

1. Introduction

The telecommunications sector in Nigeria is presently conflicted. The attendant characteristic features of a toddling industry notwithstanding. Even where an eventual self-regulated[2] and competition driven telecommunications market have been legislated into law. The industry is still, as will soon manifest, some substantial distance away from actualising this goal.

Highlight of the lingering confusion and seeming regulator-cum-operator collaboration vacillates between persistent high tariff charges and raging interconnection disputes. The consumer is confronted with a persisting situation where he grapples with multiple telephone handsets to enhance his ability to communicate. Furthermore, the user is unavoidably subjected to cope

---

1 Nigerian Communications Act, 2003.

2 S.89 sub-section 3, para. F

with network failures and sub-standardness in quality of services. Even when the services are seamlessly available, they are hardly affordable.

In a promising and diversified economy, a sustained competitive telecommunications market should represent a growing source for economic development. Above all, it must guarantee the availability of basic and affordable telecommunications services to users.

Nigeria is a federation with thirty-six states and a Federal Capital Territory, Abuja. These states represent a total of seven hundred and seventy-four local government areas. In Nigeria's present democracy[3], which is also the fourth republic[4], governance is undertaken by the three tiers of government viz. federal, state and local. Except the first republic which was a parliamentary system, successive governments[5] have been styled on the American presidential system of government with the president as head of state and head of government. While the president and his cabinet constitute the executive arm of government, the legislature is bi-cameral at the federal level. The National Assembly comprises of the Senate and House of Representatives. At the state level, it is a uni-cameral legislature symbolised by the House of Assembly. The Judiciary made up of the Supreme Court, Federal Court of Appeal, Federal High Court, and state High Courts[6]. Others include the Sharia Court of Appeal and the Customary Court of Appeal.

These organs of government are constitutionally obligated to comply with basic principles enunciated under separation of powers as well as observe necessary checks and balances. With a population of about 133 million and an area of approximately 923,768 sq km, Nigeria stands as the most populous country in Africa.

Exploration and exportation activities in the nation's crude oil deposits began to receive greater attention in the seventies under the military regime. However, the earnings from the oil sector over time have only diminished governments' attention to the economic relevance and viability of other sectors such as agriculture where the country is equally endowed.

---

3 Civilians regimes: Oct.1, 1960-Jan.15, 1966; Oct.1, 1979-Dec.31, 1983; August 26, 1993-November 17, 1993 (transition government); May 29, 1999-May 29, 2003; and May 29, 2003-date. Dates not indicated represent 29 years of Military rule since the country's independence from the United Kingdom in 1960.

4 Commonly refers to periods governed by democratically elected civilians since independence.

5 First republic as well as government at independence (0ct.1, 1960 to Oct. 15, 1966) was based on British-style Parliamentary system of government distinguishing the offices of head of state and head of government.

6 Federal High Court and state High Courts both have co-ordinate jurisdictions except in matters where FHC is constitutionally required to exercise exclusive jurisdiction e.g., the Nigerian Communications Act, 2003.

Large scale corruption, political restiveness and poor macro economic management by the government have accounted substantially for the country's persistent economic malaise.

Furthermore, the geographical inertia and persistent neglect of the rural areas by successive governments in Nigeria have combined to impose the brunt of over-population on the major cities. It is not in doubt that commercial activities and related programs facilitate the transformation of rural areas and non-major cities alike. Communication is particularly essential in that equation. The present Telecommunications legislation is an acknowledgement of the necessity of communications. With its population, oil revenue and even potential wealth from its natural resources, could a liberalised telecommunications market enable the country turn its fortunes around?

In that regard therefore, this paper has made an attempt to present an overview of the Nigeria telecommunications sector. We have noted the intrigues and market interplays which are untoward to the market. The manner in which they undermine the overall policy intendments for the fledging sector is considered. Legislative steps towards confronting these challenges in the face of an overwhelming dynamism which typifies the Information and Communications Technology have been outlined.

The benchmark for this assessment is a competitive and consumer-friendly market. Where there exists the possibility of actualising the ends of an orderly telecommunications sector, guaranteeing the eventual realisation of consumers' expectations as well as accommodating the operators' corporate goal.

The paper is divided into five sections. The first section is the **introductory** note. The market is presented at a glance under the **operating environment** in section two. The country's **telecommunications policy and laws** will form the basis for discussions in section three. The role of **regulatory authority and** ancillary **regulatory agents** has been considered in section four. The paper ends with considered views on a few **regulatory conundrums** which are closely followed by a **concluding note**.

2. The Telecommunications Operating Environment

It was not until 1999 that the government took concrete steps to implement its policy on liberalising the telecommunications market. Shortly afterwards, licences were issued to interested operators for the provision of global services for mobile communications(GSM), fixed wireless access(FWA) and fixed land lines among others. Before this period, the government-owned Nigeria Telecommunications Limited (NITEL) maintained substantial mo-

nopolistic clout in the provision of telecommunications services. Created in 1985[7] by a military government's fiat merging Nigeria External Telecommunications (NET) with the Telegraph section of Department of Post and Telegraphs(P&T).

Presently, there are four major digital mobile licensed operators[8], two national carriers[9] and several other private telecommunications operators[10] in the country.

By virtue of their operating licenses, the operators' primary obligations include the facilitation of any to any communications in the underserved population. Government and consumers expected operators appreciate the obligations under digital mobile license (DML) agreements as well as those of interconnection agreements. All of which would have added up to support well meaning efforts to remedy the present anomaly of less than 500,000 functional lines for a population of more than 133 million people.

However, the yearnings and widening disparity between the population and the number of people who had access to telecommunications services remained a cause for concern. Even when services were provided, they were concentrated only in a few cities. Poor telephone density and an accompanying dismal geographic penetration of telecommunications services to other places including rural areas, was still unresolved. This is notwithstanding the presence of NITEL, MTN, M-tel, Econet Wireless and numerous PTOs as service providers in the country's telecommunications market.

It was in an apparent bid to remedy the situation that government approved the licensing of a second national carrier. The Nigeria Communications Commission (NCC) thereafter commenced formal processes that culminated in the auction and issuance of an operating license to Global Communications Limited (Globacom) in 2002 as the second national carrier (SNO). An operating license that cost Globacom 200 million USD. A remarkable shortfall compared to 285 million USD paid each by MTN and Econet to procure the digital mobile operating license.

The SNO is expected to augment and compete with NITEL on the services provided by the national carrier.

---

7 1985 budget speech.

8 MTN Nigeria Ltd, Econet Nigeria Ltd, M-Tel (a subsidiary of NITEL), and Globacom Ltd.

9 NITEL and Globacom. While NITEL, first national carrier is owned by government, Globacom is a private company as well as the second national carrier.

10 These include: Multilinks, Reliance Telecom, Starcomms, Cellcom Limited, Bourdex Telecoms, EMIS Telecoms, 21st Century Technologies, General Telecom & Electronic, Intercellular, Startech Connections, O'dua Telecoms, Swift Networks and Cyberspace.

One significant difference is, while NITEL which is the national carrier is fully owned by the government, Globacom is a private company without any government interest.

For an optimum impact on teledensity, the SNO is authorised to provide services in the range comparable to those capable of being provided by NITEL. These include services such as the global service for mobile communications (GSM), fixed land lines, fixed wireless access and national gateway. It also means that it would meet a progressive roll-out target obligation of 150,000 fixed lines in twelve months, 550,000 lines in thirty-six month and 1,200,000 lines in sixty month. The utilisation of its installed exchange capacity should at least be eighty percent.

After some reasonable period, the SNO rolled-out its services on the 28th of August, 2003. The SNO has promised the provision of world class services and features to Nigerian consumers.

For NITEL, there is a realisation that much is required if it must meet the least expectations of the consumers without mentioning conformity with operational standards.

Lack of transparency, gross inefficiency, poor maintenance and use of outdated equipments accounted for government's earlier attempt to privatise the national carrier by selling 51% of the company's shares. The process was designed to produce a core investor in the ailing telecommunications company. The Investors International Limited emerged as the preferred bidders. However, their inability to make the mandatory deposit made the government revoke the offer.

Pending the final decision on the fate of NITEL in continuing consultations and considerations on the issue of privatisation, the government appointed a Dutch firm, Pentascope International as the management contractor. The management contractor is expected to re-position NITEL on a platform where it can confront the challenges posed by recent market liberalisation. It will also be responsible for the strategic operations of its digital mobile subsidiary, M-tel to which NITEL's digital mobile license was recently transferred.

Among the immediate task of the new team at NITEL would include debunking an impression of dissatisfaction from the consumers. Especially of note is the experience of consumers during the first year of service provisions by the digital mobile operators, MTN and Econet.

A glimpse of the persistent frustration on NITEL's inability to meet its service provision obligations was reflected in a comment that "NITEL is more of a footnote in the Nigerian GSM market". The commentator went on to note that "it is the network that should take the blame for the raw deal that GSM users are getting from the operators for if NITEL had taken off when MTN and Econet started, its charges would have made these two to

give Nigerians a better deal or face the misfortunes of lack of patronage…what Nigerians want is quality communications at affordable cost"[11]

The emergence of these operators in the wake of market liberalisation is yet to realistically impact the dismal telephone density.

Though, the fixed wireless access (FWA) providers under the local loop domain have continued to make inroads in the market while sustaining efforts in telecommunications service provision. Some have already introduced and invested in code division multiple access (CDMA) technologies to strengthen their ability to fast data access in addition to traditional voice services.

In a resolve to encourage the operators to invest in new technologies which will facilitate improved services, the government reduced import duty on telecommunications equipments from 25% to 5%. In spite of this however, the operators recognised the need to hurriedly maximise the gains obtainable from a sector without defined laws that were in full force. Even at the detriment of the consumers.

3. Telecommunication Policy and Legislations

3.1 The Wireless Telegraph Act[12]

The WTA was enacted on July 1, 1966. It was the only legislation available to both government and designated regulating authority for the regulation of telecommunications in Nigeria at the time of market liberalisation in 1999. For the regulatory authority, the WTA provided utility functions at such stages where there were needs for clarifications and referencing.

The legislative rationale under which the WTA was enacted was of course oblivious of the technological transformations that have so far attended the sector and still continuing.

The inadequacy of the WTA became more compelling considering the fact that its enactment took place when government exercised absolute monopoly in the provision of telecommunications services in the sector. This is particularly discernable from the provisions of the legislation which had vested on the Minister discretionary powers to grant and renew licences. With a proviso however requiring notice in writing when revocation is in issue[13].

---

11 Azuka Onwuka: GSM, Searching for the best connection. Thisday (28/10/02) Vol.8, No.2745, page47.

12 Chapter 469 Laws of the Federal Republic of Nigeria (LFN)

13 S.6(1),(2) and (5) of WTA

A further inconsistency with present day realities is found in its section 9 where the Minister was conferred with powers to make regulations, a function forming part of statutory mandate of the regulatory authority.

Perusing the four parts and thirty sections of the Act, the preliminary provisions outlining its short title is found in section 1.Definitions were contained in section 2 while the interpretations to the Act is found in section three, all forming contents of the first part.

The second part of this Act deals with regulation and accordingly was simply labelled in like manner.

With its nine sections, the provisions were successively arranged between section four and section twelve on issues pertaining to:

- Licence required for use of wireless telegraphy apparatus
- Licence required for dealing in wireless telegraphy apparatus
- Grant of licences
- Fees and charges for licences
- Experimental licences
- Regulations as to wireless telegraphy
- Misleading messages and interception and disclosure of messages
- Territorial extent of preceding provisions
- Powers of minister as to wireless personnel

Provisions as to interference were considered in the third part of the Act which was delimited into four sections address issues relating to:

- Regulations as to radiation of electromagnetic energy, etc[14]
- Enforcement of regulations as to the use of apparatus[15]
- Enforcement of regulations as to sales, etc. by manufacturers and others[16]
- Deliberate interference[17]

The final and concluding part[18] of the Act has fourteen sections containing general provisions. Arranged between section seventeen and section thirty, it addressed issues pertaining to penalties, offences by bodies' corporate, forfeiture, offences continued after conviction, civil proceedings, entry and search of premises etc. It also dealt with provisions applicable on an occasion of emergency, issues on onus of proof, saving as regards distress signals and

[14] S. 13
[15] S. 14
[16] S. 15
[17] S. 16
[18] Part IV

electrical apparatus, protection of government and public officers, service of notices by post, miscellaneous regulations, government sound and television broadcasting services as well as validity of previous licences.

Furthermore, it was not exactly indicated how the WTA was to address issues under a deregulated or liberalised telecommunications market.

The inherent difficulties in adapting and applying the WTA to address the rapid technological developments required governmental response. Such consideration encouraged the initiatives which were ultimately articulated under the National Telecommunications Policy.

3.2 National Telecommunications Policy

The National Telecommunications Policy captures the government's objectives and plan of action as an initial response to the unfolding challenges and innovations in the sector. The NTP maiden edition was published in 1998 and launched in October 1999. It was further reviewed and finally approved in February 2000 by the Telecommunications Sector Reform Implementation Committee.

After a prolonged absence of an enforceable legislation in the light of the current market situation, the NTP provided a tip as to the intentions of the government. Without doubt, it was a formidable platform for progress.

In the preamble, the NTP committee had noted that "the availability of an efficient, reliable and affordable telecommunications system is a key ingredient for promoting rapid socio-economic and political development of any nation" while stressing that "such a system must be universally accessible and cost-effective"[19]

The government policy goals, according to the committee, favours total liberalisation, competition and the private sector-led growth of the telecommunications sector. These were encapsulated in the NTP's short and medium term objectives.

The need to address the significant shortfall in the availability of telecommunications services to majority of people received the initial attention under the short-term objectives of the NTP. It specifically recognised the ITU recommended minimum teledensity of 1 telephone to 100 inhabitants. In other words, this meant that a target of approximately two million fixed lines and 1,200,000 mobile lines was to be reached and exceeded in two years. Though current claims on the number of users in each network by the operators lead to a conclusion of closeness to the target. This is notwithstanding the fact that preponderance of opinion think otherwise. Especially due to the

[19] National Telecommunications Policy, page 10.

inability of many users to enjoy the basic any to any communication on these networks.

One of the stated objectives of the NTP was to make conditions necessary for the country "to participate effectively in international telecommunications activities in order to promote telecommunications development in Nigeria, meet the country's international obligations and derive maximum benefits from international cooperation in these areas"[20].

Another concern discernable from the policy was to review and update telecommunications legislations so as to bring the telecommunications operators effectively under the control of the regulatory authority.

On the medium term objectives, they were not completely different from what had been outlined under the short term objectives. Though, a particularly exceptional provision was made towards ensuring that public telecommunications were accessible to communities in the country[21].

From this provision, the rationale for according the universal service obligation a secondary attention under the governments telecommunications policy outline remains unclear. This fact being particularly worrisome since an implementing authority would not see an urgent need to enforce provisions outside primary or short term goals.

When considered in context however, this probable inference had already been countered in the NTP's introductory paragraph. It stated that the country's telecommunications policy overriding objective was "to achieve the modernisation and rapid expansion of the telecommunications network and services. This will enhance national economic and social development, and integrate Nigeria internally as well as into the global telecommunications environment. Telecommunications services should, accordingly, be efficient, affordable, reliable and available to all"

This is a reiteration of the declarations under the fundamental objectives and directive principles of state policy in the constitution which provides that "the state shall direct its policy towards ensuring the promotion of a planned and balanced economic development"[22].

One caveat however is that all provisions outlined under the fundamental objectives and directive principles of state policy are however, not justiciable[23]. They cannot be contested in any Nigerian court of law.

---

20 NTP, page 24.

21 National Teleommunications Policy, page 25.

22 S. 16 sub-section 2, Constitution of the Federal Republic of Nigeria Constitution, 1999.

23 S. 6 sub-section 6 paragraph C

3.3 Nigerian Communications Act, 2003

Legislative efforts and processes to confront the dynamic challenges in telecommunications sector culminated in the signing into law on the 8th of July, 2003, the Nigerian Communications Act.

An enactment of the National Assembly, the NCA has ushered in a new era for the chaotic telecommunications market in Nigeria. Matters connected with regulations and administrations of the sector have been carefully provided for under the new law.

The passing into law of NCA has presumably re-oriented the telecommunications operators on the need to appreciate the import of certain obligations such as the universal service.

It has equally empowered the consumers by providing means to register their grievances and effectively seek redress. To safeguard the basic ends of the Act, the courts are expected to review decisions by the regulatory authority on appeal by an aggrieved person.[24]

In its explanatory memorandum, it was provided that the new telecommunications legislation repealed an earlier Act which had established the Nigerian Communications Commission.

Under the NCA, the NCC was specifically reformed as an independent regulatory body. The NCA also established the National Frequency Management Council as well as providing for the establishment of Universal Service Fund.

4. The Regulatory Authority and regulatory agents

4.1 Nigerian Communications Commission

Regulating the telecommunications sector was the main reason for establishing the Nigerian Communications Commission by the Federal Military Government in 1992 through Decree No.75 as amended[25].

As an independent regulator, the regulatory abilities of NCC have been particularly challenged between the inception of telecommunications market liberalisation and present day sector demands. Considering consumers dissatisfaction with the operators and regulators as well as the system of regulation since liberalisation, the NCA readily provides a remedy. It would among other things act as a guide in matters of procedure in seeking legitimate and effective redress in regulatory and related issues.

---

[24] S. 88 of Nigerian Communications Act, 2003.

[25] Amended by Decree 30 of 1998; now an Act of the National Assembly.

With the repeal of the legislation establishing the Commission's under the current Nigerian Communications Act,[26] the new law went a step further in strengthening the NCC in the face of recent market expectations. The legislation did not only reform the NCC, it substantially expanded its role and conferred more powers to the Commission as well.

Under its section 4, the new legislation outlined the main functions of NCC. It captures the essentials of how regulatory activities could guarantee a socially responsive and competitive telecommunications sector. These basic functions were stated as follows:

- The facilitation of investments in and entry into the Nigerian market for provision and supply of communications services, equipment and facilities[27]
- The protection and promotion of the interests of consumers against unfair practises including but not limited to matters relating to tariffs and charges for the availability and quality of communications services, equipment and facilities[28]
- Ensuring that licensees implement and operate at all times most efficient and accurate billing systems[29]
- The promotion of fair competition in the communications industry and protection of communications services and facilities providers from misuse of market power or anti-competitive and unfair practices by other services or facilities providers or equipment suppliers[30]
- The development and monitoring of performance standards and indices relating to the quality of telephone and other communications services and facilities supplied to consumers in Nigeria having regard to the best international performance indicators[31]

Furthermore, the provisions of the NCA are more of a re-statement of the founding objectives and functions of the NCC, especially in re-affirming its independence. It particularly demonstrated government's determination to realise the telecommunications sector's growth and other objectives as specified under the National Telecommunications Policy. The new law however, made considerable effort to proffer a panacea to the ineffectiveness of NCC. The practical realisation of these goals by NCC would obviate or substan-

---

26 Section 3 of Nigerian Communications Act, 2003.
27 S. 4 sub-section A
28 S. 4 (b)
29 S. 4 (c)
30 S. 4 (d)
31 S. 4 (h)

tially reduce a consumer's need to embark on an otherwise capital intensive exercise of seeking redress in court.

The above reflects the import of monitoring and reporting under section 89[32] conferring the Commission with sweeping powers to monitor all significant matters relating to the performances of all licensees while ensuring compliance to the requirement of publishing annual reports thereon at the end of each financial year. The regulator's extensive powers as contemplated in this regard would further be linked to:

- The operation and administration of the Act[33]
- The efficiency in which licensees provide facilities and services[34]
- The quality of services[35]
- Industry statistics generally including but not limited to service provisioning, traffic patterns, industry operators etc[36]
- The tariff rates and charges paid by consumers for services[37]
- The development of industry self regulation[38]
- The adequacy and availability of services in all parts of Nigeria[39]

Among the issues expected to form part of Commission's primary focus in carrying out its monitoring duties are those acts which are prohibited under the law. For example, under the new legislation, a licensee is not allowed to enter into any understanding, agreement or arrangement whether legally enforceable or not which provides for any of the following:

- Rate fixing[40]
- Market sharing[41]
- Boycott of another competitor[42]
- Boycott of a supplier of apparatus or equipment or[43]
- Boycott of any other licensee[44]

---

32 S. 89 (1) Nigerian Communications Act, 2003
33 S. 89 (3)(a)
34 S. 89 (3)(b)
35 S. 89 (3)(c)
36 S. 89 (3)(d)
37 S. 89 (3)(e)
38 S: 89 (3)(f)
39 S. 89 (3)(g)
40 S. 91 (3)(a)
41 S. 91 (3)(b)
42 S. 91 (3)(c)
43 S. 91 (3)(d)
44 S. 91 (3)(e)

Incidence of tie-in or related arrangements also tantamount to a contravention of the Act.

Specifically invalidating such actions or similar activities, the Act had specified that "a licensee shall not at any time or in any circumstance, make it a condition for the provision or supply of a product or service in a communications market that the person acquiring such product or service in the communications market is also required to acquire or not to acquire any other product or service either from himself or from another person"[45]

A lacuna in the legislation however is the absence of a specific standard for the evaluation of market dominance. Conferring discretionary power to NCC for the determination of dominant position[46] could in the long-run stifle competition as well as negatively impacting on market contrary to what the law had anticipated. In effect, this subtle threat to competition as between indeterminate strengths will continue to build especially in a situation where the Commission had been very accommodating of the excesses of the operators.

But as a post-operative requirement, the monitoring and reporting mandate of NCC will largely constitute a yardstick for evaluating the success or otherwise of the reformed regulator.

4.1 Federal Ministry of Communications

The Ministry of Communications formulates broad telecommunications policy for the country. This government department ensures that practise and regulation in the telecommunications sector conform to the overall policy objectives of the government. It particularly monitors the implementation of the National Telecommunications Policy.

In addition to formulating telecommunications policies, it would continually be required to articulate policies especially for the rapid realisation of Universal Service as contemplated under the NTP.

The new telecommunications law had outlined the under mentioned as forming part of the specific functions of the Ministry of Communications.

- The formulation, determination and monitoring, of the general policy for the communications sector in Nigeria with a view to ensuring amongst others, the utilisation of the sector as a platform for the economic and social development of Nigeria[47]

---

45 S. 91 (4)
46 S. 92 (1)
47 S. 23 (a)

- The negotiation and execution of international communications treaties and agreements, on behalf of Nigeria, between sovereign countries and international organisations and bodies[48] and
- The representation of Nigeria, in conjunction with the Commissions, at proceedings of international organisations and fora on matters relating to communications[49].

In practice however, the Ministry of Communications while acting as a supervisory ministry to the regulator do intervene in certain situations where the Nigerian Communications Commission appear to be having difficulty in making significant progress. A particular instance was recorded during the initial interconnection impasse between NITEL and two GSM operators[50] shortly after the issuance of digital mobile operating licence to the latter.

In that particular instance, it was evident that while the intractable situation worsened, NITEL still basked in its antecedent monopolistic clout leaving NCC confounded. For the NCC, the problem was not the absence of a specific solution; rather it was lack of ability to demonstrate requisite resolve as well as relying on its inherent powers under the law.

The agreement and understanding reached between the conflicting operators exemplified the regulatory influences which similar circumstances compel.

Besides, a tacit recognition of certain regulatory powers as ceded to the Ministry is statutorily supported in the NCA where it stated that "the minister shall, in writing, from time to time notify the commission of and express his views on the general policy direction of the Federal Government in respect of communications sector"[51].

These policy initiatives refer to general performance and appraisal of telecommunications service provisions both in domestic market as well as regional or trans-national regulatory endeavours.

The Ministry through the NCC maintains a network of co-operation with regional and international regulatory bodies especially the:

- Commonwealth Telecommunications Organisation
- African Telecommunications Union
- International Telecommunications Union
- West Africa Telecommunications Association

---

48 S. 23 (b)
49 S. 23 (c)
50 MTN and Econet
51 S. 25 (1) NCA

Recent initiatives by WATRA are being aimed at a single and liberalised telecommunications market within the Economic Community for West African States (ECOWAS) sub-region. It would ultimately form a platform for formal cooperation at the regional level. These would facilitate activities relating to consolidation of plans for the adoption of uniform legislation and also stimulate coordinated efforts in addressing domestic regulatory and interconnection disputes. This trans-national arrangement would equally ensure that telecommunications practices in member countries conform to international best practices while reflecting sector regulatory expectations.

4.3 The National Assembly

Under the law, legislative powers were vested in the National Assembly[52]. Its principal function is to make laws. This law-making responsibility particularly covers all matters falling under the exclusive legislative list[53] of the constitution. In addition, it shares concurrent legislative powers with states Houses of Assembly when expedient, especially on laws relating to matters under the concurrent legislative list[54].

The National Assembly, symbolising the legislature at the federal level, comprise of the Senate and the House of Representatives. In law making process, a bill may originate from either the Senate or House of Representatives. Such a bill is subsequently subjected to prescribed legislative procedures. On the completion of the specific passages, it is sent to the President for assent. The President of Nigeria will thereafter sign the bill into law upon presentation and due consideration.

At the state level, the uni-cameral legislature is adopted instead. Though, there is appreciable similarity in the law-making process. A state House of Assembly nurtures a bill in accordance with legislative requirements and processes until it is signed into law by the governor of the state[55]

Generally, legislations give force of the law to well meaning and widely supported government policies. The lawmakers through instruments of the law advance the realisation of socio-economic needs of those whose interests they represent. Though, in a place where elections are rigged with effrontery, such an assertion will at best remain a presumption. Notwithstanding, a learned writer had observed that "legislation is the most important instrument of legal development. He stated further that "it has a tremendous effect on all the other sources of law". Reason being that "it can readily alter their

---

52 S. 4 (1) Constitution of the Federal Republic of Nigeria, 1999

53 Part 1, second schedule, CFRN, 1999

54 S. 4 (4)(b), CFRN

55 S. 100 CFRN, 1999.

content", according to the writer. More importantly, the learned writer maintained that it can also be a useful tool for the social, economic and technological development of the country"[56].

The recent trend in technological developments and dynamism which awakened the Nigerian telecommunications market has remained unprecedented. The upsurge in consumers demand for telecommunications services which attended the market liberalisation remained unfulfilled. For the operators, playing without rules provided immense opportunity to recoup their investments especially, the license costs and other initial operating expenses. For the consumers, the continuing high tariffs and unruly pattern of business practices prevalent in the market remained frustrating. The passage of time only revealed the need for government's intervention. The processes which commenced with the telecommunications market liberalisation challenges culminated in the enactment of the Nigerian Communications Act, 2003.

Beyond making laws, the National Assembly participates in the ordinary government business of ensuring that these laws are implemented in accordance with overall policy objectives. They ensure that the ends of law are attained for the overall benefit of the society. Their investigative powers have been statutorily affirmed under the constitutional provisions. For example, it is constitutionally specified that "each House of the National Assembly shall have power by resolution published in its journal or in the official gazette of the Government of the Federation to direct or cause to be directed an investigation into:

a. Any matter or thing with respect to which it has power to make laws; and
b. The conduct of affairs of any person, authority, Ministry or government department charged, or intended to be charged, with the duty of or responsibility for:-

(i) Executing or administering laws enacted by the National Assembly and
(ii) Disbursing or administering moneys appropriated or to be appropriated by the National Assembly"[57].

A state House of Assembly is empowered with same legislative oversight under section 128 of the Constitution.

---

[56] Obilade A.O, the Nigerian Legal System, pg. 67; Spectrum Publishers, 2002

[57] S. 88 (1)(a) and (b) CFRN, 1999.

In like manner, an earlier provision had allowed for the formation of House Committees in each House to handle specific assignment that may be assigned to it[58].

A combination of these powers explains recent invitations extended to operators of global services for mobile communications (GSM). The Senate Committee on Communications and Commerce has resolved to take a critical look at the activities of the GSM operators in the country. The high tariffs on services and frustrations of the consumers were, according to the lawmakers, a rip-off and must be discouraged. While they maintain an oversight in the sector, the NCA will enable the lawmakers walk side by side with those whose pre-occupation it is to discern their intentions that is, the judiciary.

4.4 The Courts

Case law has been an important source of Nigeria law. There is a constitutional stipulation for hierarchy of courts in Nigeria to facilitate its legal development. An important feature of the legal system reflecting its common law influence is the time honoured application of the doctrine of binding judicial precedent. It presupposes the recognition by courts of decisions made by superior courts[59]. That is, treating previous decisions of superior courts with respect as well as referring to them in subsequent cases.

In the hierarchy of courts, the Federal High Court ordinarily shares coordinate jurisdiction with state High courts. Exceptions would however arise in situations where the FHC has been specifically thrust with exclusive jurisdiction to handle specific matters. A typical example is as provided under the Nigerian Communications Act. The FHC in addition do exercise exclusive jurisdiction on civil causes and other matters as constitutionally specified[60].

Ordinarily, appeals from the FHC lie at the Federal Court of Appeal just like appeals from the High Courts. Thereafter, appeals from FCA will lie at the Supreme Court. Matters emanating under the NCA would equally conform to this arrangement as well.

The Supreme Court of Nigeria is the apex court of the land. It is at the SC that all legal disputes are finally decided. It is at that level that the law is given its final interpretation. A feature which concurs with a learned Justice of the SC who had remarked that they were final not because they were infallible rather; they were infallible because they were final.

Under the Nigerian Communications Act, the Federal High Court was conferred with the exclusive jurisdictions over matters connected with the

---

58 S. 62 (1) CFRN, 1999

59 S. 6 (5) CFRN

60 S. 251 CFRN

Act[61]. In enforcing and observing the enforcement of the Act, everyone has a chance of participation. Accordingly, the Act stipulates that a person or the Commission could seek legal redress against any conduct prohibited by the Act under Part 1.This part specifically deals with issues connected with 'general competition practises' encapsulated between section 90 and section 94 of NCA.

However, a provision which appears to partially oust the jurisdiction of the court is found in sub-section 3 of section 88 where it provides that an aggrieved person is not expected to go to court except the aggrieved person has exhausted all the remedies provided under the Act.

On the contrary, the wordings of section 138 were as generous and comprehensive enough as to debunk such conclusion.

The provision states that "the Federal High Court shall have exclusive jurisdiction over all matters, suits and cases howsoever arising out of or pursuant to or consequent upon this Act or its subsidiary legislation and all references to Court or a Judge in this Act shall be understood and deemed to refer to the Federal High Court or a Judge of the said Court"[62].

The NCA has provided a catalyst for the development both of law and in the telecommunications sector. There is no doubt that red-tapism and bureaucratic bottlenecks do truncate the implementation of policy decisions as well as laws.

In Nigeria, it is near tradition now that respite has always come from the judiciary in the course of interpreting the laws. With the new telecommunications sector legislation, courts in Nigeria have now assumed a new mandate under the law. To ensure commitment by parties to obligations outlined under the Act.

A political science professor had reasoned in like manner while eulogising a jurist elevated to the bench recently. The basis was "…informed by Nigeria's recent and not-so-recent experience, that the law remains an important instrument for turning the impossible into reality, for bringing water up from the bowels of the arid desert; indeed, for engineering development out of Nigeria's current morass of incoherence, insecurity, frustrations, hunger and anger as epitomised by the current season of anomie ravaging the land".[63]

Though it is an onerous responsibility in a season of misplaced developmental imperatives, the judiciary in Nigeria will assume the task with its legendary fervour. Even if such development is realised after an avalanche of cases, the ends of policies will ultimately be honoured. For any contrary view, Kayode Eso, retired Justice of the Supreme Court of Nigeria gave a view from the highest bench. He had adumbrated that "a challenge in court …should be

---

61 S. 138

62 ibid

63 Adigun Agbaje, in honour of Oladejo Akanbi; The Guardian, August 1, 2003.

regarded as a healthy phenomenon and not a sabotage of any process, transition or permanent"[64]

Much has been achieved, but more needs to be done if policies must of necessity be translated into realities.

5. Regulatory Conundrums

5.1 Affordable price for services Vs Return on Investment.

Having paid 285 million USD for a digital mobile licence, the GSM operators have, from the period of roll-out, inexorably clung on their right to return on investment. After making a profit of about 9 million USD in a financial year, Chief Operating Officer of a GSM operator had hissed that business environment in Nigeria was very harsh. But would claim under same breathe, of colossal investments in telecommunications infrastructures and expansion costs which the operators had made and continued making.

Palliative measures by the government to make the business environment conducive for operations being highlighted. The Government had in fact started by reducing import duties on telecommunication equipments from 25% to 5%, including tax incentives and other subsidies which the operators are yet to explore.

Oblivious of the general economic impact and the essentiality of services provided by the operators, the regulator is not sufficiently persuaded by the complaints of the consumers against the insensitivity of the operators. For the regulator, there is no need to interfere with the market. It made no difference whether the features in the market can stimulate competition or stifle it. The regulator believes that since it is about service provision, market and consumers, competition would come on its own. This is despite the scepticism being expressed by market observers or the rationale inferable from the establishment of the regulatory agency by government.

In addition, were the regulators assertion correct, situations would not have compelled the country's President, prior to enactment of NCA, to dialogue with the operators on high tariff and quality of service.

If a policy was drawn up after due reflection on the need for rapid socio-economic development of a nation, its implementation should necessarily reflect those concerns. Also, as much as practicable, various implementing

---

[64] Kayode Eso,Justice of the Supreme Court(rtd) in Further Thoughts on Law and Jurisprudence, pg 244; John Ademola Yakubu (ed),Spectrum Publishers(2003)

agencies or authorities should make effort to operate with dedicated reference to the intendments of such policy considerations.

On the knotty issues arising out of the newly liberalised telecommunications market environment, the regulator will rather view it from operators' standpoint. So far, the consumer is yet to realistically feel the impact of the services being provided by these telecommunications.

For the sake of economic development which the telecommunications sector should necessarily facilitate, the regulator should map out realistic strategies for actualising the expectations of the newly enacted law. It is required to appreciate the enormity of responsibilities arising from the Act especially as they relate to:

- The exact role of a regulator under its functions in section 4 of NCA.
- The ends envisaged by the National Telecommunications Policy on issues of development and reaffirmed by the Act.

The seeming inability of the regulator to realistically confront the situation explains the restlessness of both the lawmakers and the Presidency. A growing situation that is self-defeating for NCC especially for questions on regulatory independence.

Assuming the regulator confronted the market's challenge uninhibitedly in the exercise of its mandate, the operators' excesses and utter disregard for sector policy goals would have been contained.

There is a dire need for the existence of an effective forum where representatives of government, consumers and operators would state their opinion on sector related issues. A platform where views and complaints vented would be duly considered and thereafter outline subsequent but effective means to remedy situations where required.

Pragmatic mechanisms and subsidies to accommodate the operators cost can be explored. This arrangement should not obviate the need to nurture a market where users will benefit from the technological advancement. That would basically form an essence of such legitimate endeavour. Especially as an orderly telecommunications market will bring about a multiplier effect to other sectors in the economy.

5.2 Teledensity and Universal Service

As enshrined in the National Telecommunications Policy, the NCA made copious provisions for the Universal Service[65]. Its relevance was further ex-

[65] S. 112 CFRN

pressed under section 114 of the NCA which created a Universal Service Provision Fund.

This opportunity to link the rural areas must not be defeated by government's inability to ascertain the exact number of people inhabiting the suburbs as well as the metropolis. In same manner a commentator wondered why Nigeria has remained a country where vital statistics were either unavailable or of doubtful character.

To realise the Universal Service, there is required, an effective plan for regulatory action, setting of basic service quality standards and consistent proactive monitoring. Compliance with licence agreement terms by operators as well as commitment to obligations need to be demonstrated for the realisation of universal service.

In this connection, Universal Service should be aligned with practical realisation of a 25km availability of functioning telecommunication services in the rural areas. It also contemplates both unserved and underserved areas, as well as underserved groups[66]. Only then would there be sufficient justification for reliance on figures which denote the country's telephone density for proper evaluation.

It will therefore be misleading to base the country's telephone density on telecommunications service availability in a few densely populated commercial cities where the operators presently cluster. Linking the rural areas is a sine qua non to an enduring development as envisaged under the sector policy. Such a measure will jump-start economic activities in those areas. It will in turn transform these areas while reducing the pressure on cities caused by migration especially on infrastructural amenities and social vices.

The provision of universal service is the bed-rock of government's sector goals. This has been demonstrated by the recent legislation designed to actualise the stated objectives.

It will tantamount to regulatory laxity to allow the operator dictate the pace at which the government's policy objectives will be achieved. Presuming the existence of competition in a market incapable of regulating itself is misleading. Persistent reluctance by operators to align their corporate mission and profit maximization goals to the principles enshrined in the NTP for sector growth must be discouraged.

---

[66] S. 113 CFRN

5.3 Conclusion

Behind the façade of what seems a disorderly sector lie potentials for growth, and large market in the Nigeria telecommunications industry. This is especially predicated on the nation's population, significant level of commercial activities across sectors.

The independent regulator should make genuine effort to assume the mandate thrust upon it by the Nigerian Communications Act, using both sector and economic developments as yardstick.

It should painstakingly ensure operator's compliance with contractual licence terms and obligations. Combinations of these efforts would reduce frictions among operators on one hand and between operators and consumers on another. Guaranteeing a connection to the information super-highway and seamlessly too between networks working together for common development ends.

The accompanying development benefits as well as challenges which the rapidly evolving ICT presents in the telecommunications sector should not be discountenanced as a transiting phenomenon. Neither should it be managed without regard and reference to sector policy and law. Encouraging any of these situations would mean committing the nations developing telecommunications market to the vagaries of operators' self-benefiting corporate strategies.

8 THE BRUSSELS I REGULATION ARTICLE 15.1C)

Whereto are commercial or professional activities directed through the Internet? [1]

by Georg Philip Krog[2]

I. Introduction

The Member States of the EU considered the Council Regulation (EC) No 44/2001 of 22 December 2001[3] (hereinafter "the Brussels I Regulation") as an urgent measure designed to remove the existing legal uncertainties as to the application of its' predecessor, the Brussels Convention of 27 September 1968, to e-commerce.

This legislative urgency was motivated by the jurisdictional implications of the digital information- and communication network, the Internet. Activities, interactions and business transactions increasingly straddle each country's borders through its' global, borderless and potentially uncontrollable multi-jurisdictional reach, hence forth international legal disputes of heterogonous character arise and will continue to arise in incalculable numbers. Thus, disputes arising out of the Internet will make up a significant portion of what falls within the scope of the international legal order of jurisdiction.

The authors of the Brussels I Regulation were aware of the fact that regulating Internet activities could have implications outside the intra-Community

---

1 This article was earlier this year published in IPRax.

2 *Georg Philip Krog* is a Research Fellow and candidate for the *doctor juris degree* at the University of Oslo, Norway, the Faculty of Law, the Norwegian Research Center for Computers and Law. This article was written whilst the author was a Visiting Fulbright Researcher at Harvard Law School, the European Law Research Center under the head of its´ Director, Professor David Kennedy to whom I am very thankful for making my research stay possible.

3 Council Regulation (EC) No 44/2001 of 22.12.2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, replacing the Brussels Convention of 27 September 1968, the consolidated version of which was published in the OJ C 27, 26.1.1998, p. 1. But the Brussels Convention of 1968 remains in force for relations between Denmark and the other Member States.

legal order of the EU since the Internet is not geographically limited to the EU territory. In this context, the authors of the Brussels I Regulation sought to reconcile three objectives. First to serve, promote and cultivate the growth of e-commerce in the EU. Second to ensure persons domiciled therein are not deterred from using the Internet to promote their goods and services thereby supporting competitiveness of European companies at global level. Third to guarantee the best possible legal protection for its citizens, in particular consumers, in relation to the development of e-commerce and its risks.[4]

Such a framework would allow businesses to calculate and manage the risks and costs associated with where they should be established, how to run the business operation and litigate in foreign courts as a result of their use of digital and electronic means, as well as enhance the confidence of customers.

Thus, from an e-commerce perspective, research on the conditions for determining the scope of application jurisdiction *ratione loci* is essential in order for the parties to clarify their respective rights, obligations and responsibilities.

In this regard, several provisions in the Brussels I Regulation are relevant, e.g. the scope of application *ratione loci* in relation to Art 2, 5.1, 5.3, 5.5 and 15.1c) in addition to its general scope of application.

The drafting of Art 15 provoked strong concern and debate within the business community. Several commentators, including the comment of the Economic and Social Committee, believe that Art 15.1c) and the expression ¨by any means, directs … to" is not clear enough to foster a climate of trust between the parties, and that it does not distinctly serve as a precise criterion to designate, refer and connect whereto commercial or professional activities are directed through the Internet. Thus, the author of this article has a twofold purpose.

First, the article provides an introduction to and questioning of how the scope of application *ratione loci*[5] set out in Art 15.1c) by the autonomous[6]

---

4 See Opinion of the Economic and Social Committee on the 'Proposal for a Council Regulation (EC) on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters', Official Journal C 117, 26/04/2000 P. 0006 – 0011. See also Report on the proposal for a Council regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters(COM (1999) 348 – C5-0169/1999 – 1999/0154(CNS)) Committee on Legal Affairs and the Internal Market, Rapporteur *Diana Wallis*.

5 While the first part of the Brussels Convention Art. 13 has undergone some minor linguistic amendments in the Brussels I Regulation Art. 15.1c), the expressions in Art. 13.3 of the Brussels Convention determining the *ratione materiae* "any other contract" and "for the supply of goods or a contract for the supply of services" were replaced respectively with the expressions "in all other cases" and "the contract" in addition to defining the vendor (with whom the consumer concludes the contract) as a "person who conducts "commercial or professional activities".

6 The methodology of interpretation of Art. 13 to 15 of the Brussels Convention is according to settled case-law, that the concepts therein must be interpreted independently, by reference principally to the system and objectives of the Convention, in order to ensure that it is

expression "by any means, directs … to" should be interpreted and applied to the digital environment, with a particular view to commercial and professional activities carried out through websites.

Second, the article questions whether the amendments of the old concepts in the Brussels Convention Art 13, paragraph 3, was a successful and appropriate policy reconsideration for the Member States in the intra-Community legal order of the EU pursuant to the scope of application of Art 15.1c).[7]

Art 15.1c) provides in full:

> *1. In matters relating to a contract concluded by a person, the consumer, for a purpose which can be regarded as being outside his trade or profession, jurisdiction shall be determined by this Section, without prejudice to Article 4 and point 5 of Article 5, if:*
>
> *c) in all other cases, the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities.*

The first purpose has a practical agenda. The aim is to discover, alert and awake courts, lawyers and (potential) disputing parties with crucial questions to see the content that is genuinely and ultimately at issue when interpreting Art 15.1c). The Brussels I Regulation imposes the national courts of the Member States the duty of examining whether the rules and their specific conditions for conferring jurisdiction attribute jurisdiction to the court where the plaintiff decides to sue the defendant. Thus each Member State's national procedural laws are set aside in matters governed by the Brussels I Regulation in favour of the provisions thereof. Hence, the article seeks to be sensitive to the richness of the meaning of the terms employed in Art 15.1c) in relation to the problems of applicability to the ¨new¨ phenomena of the Internet, without crystallizing them into a doctrine or technical vocabulary.

---

fully effective, see Shearson Lehmann Hutton Inc. v TVB Treuhandgesellschaft für Vermögensverwaltung und Beteiligungen mbH, Case C-89/91, European Court Rreports 1993 p 139, paragraph 13 with reference to case-law. This will eliminate obstacles to legal relations and to the settlement of disputes in the context of intra-community relations. Art. 15 to 17 of the Brussels I Regulation must be interpreted by the same methodology of interpretation, and the Preamble to the Brussels I Regulation recitals 5 and 19 emphasize the continuity between the Brussels Convention and the Brussels I Regulation.

7 This problem has, not only in the EU, but also worldwide, instigated a reconsideration of the jurisdictional principles and the question whether the scope of application of the provisions within the international legal order of jurisdiction should be amended.

This is practical in at least six respects: First, e-commerce increases, and many interactions and transactions are of international character subsequently falling in under the scope of the international legal order and the rules of jurisdiction. Second, many e-customers are consumers. Third, since it may be difficult for a vendor to identify in what capacity his customer acts (consumer or a professional), and the provisions governing consumer contracts in the Brussels I Regulation Art 15 to 17 grant the consumer a better protection (on the costs of the vendor) than the general rule of jurisdiction in Art 2 or the alternative rule in Art 5.1, it is probable that the vendor will adjust the commercial and professional operation of his website in relation to consumers and in particular Art 15.1c) in order to determine where the vendor can sue or be sued. This is substantiated by the fact that the forum country where the consumer is domiciled often must apply national mandatory consumer rules, thus setting aside the designated law, which is applicable according to the choice-of-law rules. Fourth, the provisions set out in the Brussels I Regulation Art 15 to 17 are mandatory[8] jurisdictional rules in certain situations when a contract has been concluded between a legal or natural person who conducts commercial or professional activities and a consumer, for a purpose, which can be regarded as being outside his trade or profession. Fifth, since many vendors do not operate with commercial or professional on-line platforms separate for consumers in Europe and the rest of the world, the introduction of Art 15.1c) will also imply a regulation of activities directed to territories outside the EU. Sixth, Art 15.1c) does not solely concern itself with legal relationships arising out of offers and conclusions of contracts within its territorial scope. Rather, Art 15.1 c) is concerned with the effects on the territory of the EU, regardless from where that effect was directed.[9] This implies that both offers and conclusions of contracts can origin from anywhere in the world and still fall under the scope of Art 15.1c) provided that the plaintiff is domiciled in a Member State.[10]

---

8 See Chapter II, point 1.

9 Assuming that the other party to the contract, the vendor, is not domiciled in a Member State, the question arise whether the vendor's website can constitute "[…] a branch, agency or establishment in one of the Member States […]", and whether a contractual dispute arising out of the operation of his website is a dispute "[…] arising out of the operation of the branch, agency or other establishment […]" according to the Brussels I Regulation Art. 15.2.

10 In order for Section 4 of the Brussels I Regulation to apply, the general criterion that the defendant must be domiciled in a Member State must be fulfilled. With respect to consumer contracts, the only exception to the rule in Art. 4 is introduced by the second paragraph of Art.15.2, which applies where a consumer enters into contract with a party who is not domiciled in a Member State but has a branch, agency or other establishment there and the dispute arises out of its operations. Accordingly, the courts of the State in which the consumer is domiciled have jurisdiction, in accordance with Art. 16.1, in proceedings

The key question is to examine if and how jurisdiction *ratione loci* ¨by any means, directs … to¨ in the Brussels I Regulation Article 15.1c), covering a variety and multiplicity of consumer contracts as a whole, can be construed in relation to three objectives. Firstly, how can its' scope of application ensure adequate protection for the consumer who is considered deemed to be economically weaker and less experienced in legal matters than his professional co-contractor? Secondly, how can its' scope of application establish a close connecting factor between the dispute and the court and ensure that there are close connections between the contract in issue and the State in which the consumer is domiciled? Thirdly, how can its' scope of application, as the recital (11) in the Brussels I Regulation requires, establish a rule, which is ¨highly predictable¨? In other words, how can the court deduct a rule, which is easily to identify by a normally well-informed plaintiff as well as reasonable to foresee by a normally well-informed defendant?

The second purpose has a theoretical agenda, namely to question whether Art 15.1c) *ratione loci* by the term ¨by any means, directs … to¨ is constructed and elaborated in a new set of analysis, breaking through the old structure in order to think a new with a new vocabulary fit for the new phenomena of the Internet.

The critical questioning forwarded in this article represents the author's attempt to initiate incentives for a critical revision of the Brussels I Regulation and the Lugano Convention[11], and for the current conversion of the Rome Convention of 1980 on the law applicable to contractual obligations into a Community instrument.

In order to assess whether or not Art 15.1c) and the *ratione loci* ¨by any means, directs … to¨ sets aside old concepts of legislative authoring in the Brussels Convention Art 13, first paragraph, point 3[12], which traditionally has been interpreted and applied predominantly to actions related and con-

---

under Art. 15.2 of the Brussels I Regulation, if the other party to the contract is domiciled in a Member State or is deemed under Art. 15.2 to be so domiciled, see *Wolfgang Brenner v Dean Witter Reynolds Inc.,* ECR 1994, p I/4275, paragraph 19. Hence forth, the question arises whether the operation of e.g. a website or an electronic agent constitute a "branch, agency or other establishment".

11 The Lugano Convention of 16 September 1988. Concerning the applicability of the Lugano Convention Art. 13 to e-commerce, see *Foss, Morten*, Rettslig Klassifisering av Digitale Produkter og Nettsteder – eksemplifisert ved Luganokonvensjonens Bestemmelser om Forbrukerkjøp, Complex 9/03.

12 For further reading regarding the applicability of the Brussels Convention Art. 13, paragraph 3, to e-commerce, see e.g. *Foss, Morten and Bygrave, Lee*, International Consumer Purchases through the Internet: Jurisdictional Issues pursuant to European Law, International Journal of Law and Information Technology, 2000, 8/2; *Stone, Peter*, Internet Consumer Contracts and European Private International Law, Information and Communication Technology Law, 2000, 9.

nected to the off-line world with a view to physical and geographical locations, it is first crucial to identify the amendments. Second, it is crucial to identify the particular features of the Internet and question whether the amendments are appropriate for determining the jurisdiction *ratione loci* when disputes arise out of Internet interactions and transactions.

The particular features of the Internet is that it mediates, or directs,[13] our selection of utterances (constituting the information) in various forms[14] with a specter of functions through an increasing amount of communication- and information services while offering different degrees of interactivity.[15] This mediation is, in contrast to other traditional media, often international in scope even though the people in a traditional sense do not find themselves in an international arena when they physically interact from the place where they are domiciled or habitually resident. This is because the Internet is not geographically limited to a State's territory as other channels of distribution mainly have been and, to a great extent still are. Subsequently, our selection of utterances (information) physically carried out on the territory of State X through the Internet imply a communicative action in or directed to other countries than the country from where the person active on the Internet physically acts since the selection of utterances constitutes information and generates a memory, which may have information value in those countries where the information is understood, not by duplication of the information, but rather by selective understanding. The synthesis of the three different selections of information, utterance and understanding/misunderstanding mutually presupposes that the information is the cause of the utterance and the utterance is the cause of the understanding and the understanding is the cause for a new utterance. This means that there is a system of communication, and that there is no information outside of communication, no utterance outside communication, no understanding outside of communication. These three selections are causal preconditions for (international) interactions and transactions through the Internet, after which the rules of law may accentuate one side or the other (see Chapter II point 3) and thus either emphasize the reason for which the information is uttered (e.g. purposefulness in relation to various fields of law, or was a contractual acceptance made), the information itself (e.g. trademarks) or its content value for other persons (was a contractual offer made). It follows that the elements of disputes arising out of communicating

---

13 Between private individuals, and private individuals and other legal entities.

14 E.g. sound, text, still pictures, motion pictures, multimedia.

15 Active as well as passive reception. This stands in contrast to traditional media where international interactions between individuals were conducted by telephone, which by its' nature, limited the number of interacting individuals, or television, which by its' nature to a great degree limited individuals' possibility to actively interact and was a carrier for passive reception of information from a company to individuals.

information through the Internet have fairly unclear physical geographical reference points to national and sub-national boundaries, which in turn makes it problematic to appoint the relevant connecting factors for asserting jurisdiction and thereby make clear jurisdictional rules.[16]

More concretely - taking the example from the Green Paper (on the conversion of the Rome Convention of 1980 on the law applicable to contractual obligations into a Community instrument and its modernization) - a Greek consumer who bought an electronic instrument in Germany […] via the Internet […] wants to sue the manufacturer because it has a serious defect that the manufacturer refuses to repair […].[17] Applying the new vocabulary of Art 15.1c) ¨by any means, directs … to¨ to the global, borderless and potentially uncontrollable multi-jurisdictional reach of the Internet, how and by what precise criteria can the German vendor foresee whereto his commercial or professional activities are directed? How can the court, where the Greek consumer sues, delimit and localize the legal relationship in the sphere of a jurisdiction and determinate the attribution of competence to court to adjudicate the subject matter by as far as possible a unitary application of the jurisdictional rules?[18]

This article concludes that it is not certain what one can deduct from the terms "by any means, directs … to" in Art 15.1c), and that Art 15.1c), as it stands with its sources of law, does not establish legal certainty. The reason is twofold. First, the ECJ has so far not given any interpretations.[19] Second, the preparatory works are on many points ambiguous as to the autonomous understanding of the terms "by any means, directs … to" in Art 15.1c), especially regarding its application to e-commerce. The Commission gave an initial proposal[20] and an amended proposal.[21] The latter rejected the proposals

---

16 By contrast, the off-line world, with steady, physical geographical reference points designates rather clearly connections to specific territories (as in the case of e.g. traffic accidents) thereby making it rather uncomplicated to appoint the relevant connecting factors by which jurisdiction can be attributed to court.

17 See the Green Paper, on the conversion of the Rome Convention of 1980 on the law applicable to contractual obligations into a Community instrument and its modernization, Brussels, 14.1.2003, COM (2002) 654 final, p 5, point 1.1.

18 Subsequently excluding all other potentially competent courts other than the one designated in order to avoid multi-jurisdictional and often simultaneous competing competence to exercise jurisdiction pursuant to consumer contracts.

19 The sources of law are limited to the earlier case-law regarding the Brussels Convention Art. 13 and 14.

20 Proposal for a Council Regulation (EC) on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters /* COM/99/0348 final - CNS 99/0154 */ Official Journal C 376 E, 28/12/1999, p. 1-17. Here the Commission proposed in Recital 13 that: "(13) Account must be taken of the growing development of the new communication technologies, particularly in relation to consumers; whereas, in particular, electronic commerce in goods or services by a means accessible in another Member State

forwarded by the Parliament[22] stating that the Parliament's definition of the concept of activities directed towards one or more Member States ran counter to the philosophy of Art 15.[23] Also, the preparatory works refer and reason with the terms "interactive" and "passive" websites without clarifying the content and differences of those concepts. [24]

It follows that the interpretation of the terms "by any means, directs … to" in Art 15.1c) must be conducted in accordance and compliance with the general methodology of the ECJ with particular regard to the special objectives proper to Section 4, and the general objectives of the Brussels I Regulation, deducted from its scheme and system.

Further, it is this author's opinion that with the technological advances of the Internet, the legislative authors of the Brussels I Regulation should reconsider the semantics in relation to the conceptual frames of physical reference points, and provide new criteria to unfold the paradoxes inherent in all distinctions that are used for determining jurisdiction *ratione loci* pursuant to this global digital network. Otherwise, communication through networks with a global reach might be considered too risky with probabilities of lawsuits in foreign countries. Henceforth the one who utters something and the one who understands something of the utterance and utters, either back or to someone else, might avoid communication, which in the end may be a condition for no further access to information and communication.

It follows that the author in the subsequent section solely will discuss jurisdiction *ratione loci* and the expression ¨by any means, directs … to¨. It follows that the author refrains from commenting on the three general requirements of what constitute a "contract" [25] [26], "consumer"[27] and "a person

---

constitutes an activity directed to that State. Where that other State is the State of the consumer's domicile, the consumer must be able to enjoy the protection available to him when he enters into a consumer contract by electronic means from his domicile."

21 Amended proposal for a Council Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (presented by the Commission pursuant to Article 250 (2) of the EC-Treaty)/* COM/2000/0689 final - CNS 99/0154 */ Official Journal C 062 E , 27/02/2001, p. 243–275.

22 EP opinion 1st reading Proposal for a Council regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (COM (1999) 348 - C5-0169/1999 - 1999/0154(CNS)) C 146 (2001), p. 94–101.

23 See paragraph 2.2.2 of the Amended proposal for a Council Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (presented by the Commission pursuant to Article 250 (2) of the EC-Treaty)/* COM/2000/0689 final - CNS 99/0154 */ Official Journal C 062 E, 27/02/2001, p. 243–275.

24 These concepts originated from U.S. case-law where U.S. courts for a while employed and determined jurisdiction with reference to "interactive" and "passive" websites, first in the *Zippo Mfg. Co. v. Zippo Dot Com, Inc.* 952 F. Supp. 1119, (W.D. pa. 1997), see supra note 55.

25 Regarding the relation between Art. 5.1 and Art. 15 to 17, see Chapter II, point 1.

who pursues commercial or professional activities"[28] [29]as well as jurisdiction *ratione loci* pursuant to the expression "pursues […] in the Member State of the consumer's domicile"[30].

II. Ratione loci: "by any means, directs … to"

1. Applicability of Art 15.1c) is strictly limited to the objectives proper to Section 4

It must be observed that the provisions governing consumer contracts in Art 15 and 16 are mandatory and imperative rules of jurisdiction, and therefore override, with the exception of Art 17, the applicability of any other rule.

---

[26] Since the concept of a contract varies from one Member State to another in accordance with the objectives pursued by their respective laws, it is necessary, in the context of the Brussels I Regulation, to consider that concept as being independent and therefore to give it a uniform substantive content allied to the European Community order. Therefore, it is indispensable for the coherence of the provisions to give the expression "contract" in Art. 15 a uniform substantive content. Consequently, it should be noted at the outset that the meaning of the expression "contract" is to be interpreted autonomously, and thus assumingly the same as in the general rule of jurisdiction in contracts laid down in Art. 5.1 to which a body of case-law is relevant.

[27] For further reading on the consumer requirement *see Bertrand v Paul Ott KG*, Case 150/77, European Court Reports 1978 p 1431; Shearson Lehmann Hutton Inc. v TVB Treuhandgesellschaft für Vermögensverwaltung und Beteiligungen mbH, Case C-89/91, European Court Reports 1993 p 139; *Francesco Benincasa v Dentalkit Srl.*, Case C-269/95, European Court Reports 1997 p. 03767. See also, to that effect the Expert Report drawn up when the Kingdom of Denmark, Ireland and the United Kingdom of Great Britain and Northern Ireland acceded to the Convention, OJ 1979 C 59, p. 71, paragraph 15.

[28] A natural understanding of the wording suggests that the Art. 15.1c) is meant to cover direction from the natural or legal person with whom the consumer concludes the contract. Thus, the question arise who this "person" is, whether Art. 15.1c) applies only to the person who directly or also indirectly through a third-party by contract or independently directs such activities, and how to distinguish this person from other persons who through the Internet direct the same commercial or professional activity towards a Member State?

[29] Particular problems arise when vendors collaborate to direct, or seek to circumvent being considered as the person who directs the commercial or professional activities to a Member State. Closely related and often interconnected is the question whether it is necessary and in case how to distinct one "commercial or professional" activity from another. Since many vendors conduct identical trading operations, offer the same goods and services and employ the same technical platform, design, marketing, prices etc. (generic and identical commercial or professional activities), it may be difficult to distinct this question from the former.

[30] For further reading regarding jurisdiction *ratione loci* "pursues … in", see *Øren, S. T., Joakim*, INTERNATIONAL JURISDICTION OVER CONSUMER CONTRACTS IN e-EUROPE, International and Comparative Law Quarterly, 2003, Volume 52, p. 676.

The rules of jurisdiction in Art 15 and 16 may be departed from only if there is compliance with the conditions laid down in Article 17. Art 15 to 17 must be strictly limited to the objectives proper to Section 4 of the said Regulation since Art 15 to 17 constitute a *lex specialis* in relation to Art 5.1, and subsequently derogates from the general principles of the system laid down by the Brussels I Regulation in matters relating to contract, such as may be derived in particular in Art 2 and 5.1. Such an interpretation must apply *a fortiori* with respect to a rule of jurisdiction, such as that contained in Article 15 of the Brussels I Regulation.[31]

The protection afforded the consumer in Art 15.1.c) is to grant him the privilege of not being haled into court in a foreign country.[32] Thus, it is important to have a clear understanding of the underlying policy. The purpose of the special regime introduced by the provisions regarding consumer contracts was to ensure adequate protection for certain categories of buyers, specifically for the consumer.[33] Those provisions cover only a private final consumer, not engaged in trade or professional activities, who is bound by one of the three types of contract listed in Art 15.1 a), b) and c) and who is also personally a party to the action, in accordance with Art 16.[34] Art 15 affords protection to the consumer from being hauled into court in a foreign country. The protective role fulfilled by Art 15 implies that the application of the rules of mandatory jurisdiction laid down to that end by the Brussels I Regulation should not be extended to persons for whom that protection is not justified. The reason being that the consumer as the contracting party is

---

31 Apart from the cases expressly provided for, the Brussels I Regulation appears clearly hostile towards the attribution of jurisdiction to the courts of the plaintiff's domicile.

32 The protective role fulfilled by those provisions implies that the application of the rules of special jurisdiction laid down to that end by the Brussels I Regulation should not be extended to persons for whom that protection is not justified.

33 See Chapter 4.2 of the Commission's initial proposal, supra note 17. Regarding the Brussels Convention, see *Jenard*: "Report concerning the Convention on jurisdiction and the enforcement of judgments in civil and commercial matters" (Official Journal 1979 C 59, s. 1 – 65 and s. 66 – 70) p. 33, *Schlosser* "Report on the Convention on the Association of the Kingdom of Denmark, Ireland and the United Kingdom of Great Britain and Northern Ireland to the Convention on jurisdiction and the enforcement of judgments in civil and commercial matters and to the Protocol on its interpretation by the Court of Justice" (Official Journal 1979 C 59, p. 71) p. 117, Giuliano & Lagarde "Report on the Convention on the law applicable to contractual obligations" (Official Journal 1980 C 282, p 1) p. 23, and *Bertrand v Paul Otto KG*, Case 150/77 European Court Reports 1978 p 1431, paragraph 21.

34 See Shearson Lehmann Hutton Inc. v TVB Treuhandgesellschaft für Vermögensverwaltung und Beteiligungen mbH, Case C-89/91, European Court Reports 1993 p 139, paragraph 19, 20, 22 and 24.

considered deemed to be economically weaker[35] and less experienced in legal matters than his professional co-contractor.

2. Applicable to Internet-direction?

It must be observed that the Brussels Convention Art 13, paragraph 3 and the Brussels I Regulation Art 15.1c) are applicable to the Internet even though the scope of application *ratione loci* employ different terms.

The applicability of the Brussels Convention Art 13, paragraph 3, point (a) to consumer contracts entered into through the Internet was determined by the expressions ¨specific invitation addressed to the consumer or by advertising¨. The ECJ elaborated in *Rudolf Gabriel* on these concepts stating that they "cover all forms of advertising carried out in the Contracting State in which the consumer is domiciled, whether disseminated generally by the press, radio, television, cinema or any other medium, or addressed directly, for example by means of catalogues sent specifically to that State, as well as commercial offers made to the consumer in person, in particular by an agent or door-to-door salesman."[36] Since the Internet existed at the time of the judgment, one can assume that the expression "any other medium" also refers to the Internet.

The applicability of the Brussels I Regulation Art 15.1c) is determined by the term ¨by any means¨. A natural understanding of the wording suggests that the Art 15.1c) is meant to cover all forms of direction of commercial or professional activities regardless of what has been employed. Thus, it is reasonable to conclude that Art 15.1c) does not distinguish between different forms of means and medium of commerce, and that there is no limitation as to means of direction. This suggests that all means of direction, including the Internet, must be taken into cumulative consideration when determining whether or not the vendor's activities are directed to a Member State. This is also in harmony with the general considerations of public policy, which motivated the reconsiderations of the scope of application of the jurisdictional concepts laid down in the Brussels Convention. This means that all communication- and information services of the Internet, including with no limitation the World Wide Web, e-mail, e-agents, chat, newsgroups etc are relevant in addition, but with no limitation, to other traditional channels of distribution such as ordinary mail, TV, radio, mobile and ordinary phones, fax, traditional book and newspaper publications.

---

[35] Many of the national laws incorporate the idea of protection for the customer, or the consumer, since he/she is considered as the weaker party in economic terms in comparison with the seller. Certain laws are also based on considerations of economic, monetary and other policies, which are intended to control the sales to consumers.

[36] See Rudolf Gabriel, Case C-96/00, European Court Reports 2002 p 6367, paragraph 44.

3. Does ¨directs … to¨ mean the vendor's direction of his utterance to the Member State of the consumer's domicile, or the consumer's reception and understanding of direction in that Member State, or a combination of such direction?

The article will demonstrate in the following points that the preparatory works on this point are ambiguous. Also, the wording ¨directs commercial or professional activities to the Member State of the consumer's domicile¨ is indefinite to the question. To start with, the wording does not require a presence of such an activity ¨in¨ the consumer's Member State, whether physically or by representation of e.g. binary signs in a digital network. Rather, the wording requires a "direction¨ of such activity ¨to¨ that Member State, presupposing that the action of ¨commercial and professional activities¨ is not the same operation as ¨direction¨. Therefore, it can be maintained that if a vendor's action of commercial and professional activities solely are confined ¨in¨ State A, they are not directed ¨to¨ State B. Thus, in this regard, the concept of ¨action¨ of ¨commercial or professional activities¨ is irrelevant. Rather, the meaning of ¨directs … to¨ refers to a presentation of the selection of information pursuant to ¨commercial and professional activities¨, of which this ¨direction¨ is a precondition for possible or factual conclusions of contracts. This leads to the question whether the expression ¨directs … to¨ is to be understood as only meaning the vendor's utterance of this selection of information to the Member State of the consumer's domicile[37], or the Member State's selective understanding of this selected utterance of information, or both.

It is conceivable that the first alternative can appear on its own since the vendor may present his commercial and professional activities on a website without anyone seeing it or knowing about it. However, it is only when a consumer has understood (or misunderstood) the information value of its content and the reason for which the content has been uttered that communication of selected information on the side of the vendor *and* the consumer has been generated.[38]

If a court was to determine the attribution of jurisdiction to court according to the second alternative, the court would have to consider the whole social operation of communication between the vendor and the consumer since this alternative is caused and circularly presupposed by the first. This means that the court first would have to determine the selected information the vendor utters. Second, since understanding is not a duplication of the utterance, the

[37] Often, utterances are no longer what was thought or meant.

[38] At this point it is important to distinguish communication from perception since the latter is a psychological event without communicative existence. From an external point of view, one cannot respond to what another has perceived.

court would have to determine the consumer's selective information value and his understanding of the reason for which the content has been uttered. In this perspective, information and communication is risky since a court itself can misunderstand the respective utterance and (selective) understanding of the vendor and the consumer. Moreover, it is a complicated task for a court to consider whether the consumer understood the vendor since it would bring about an assessment of causality meaning that the information would have to cause the vendor's utterance, and this utterance would have to be the cause of the consumer's understanding. In such a causality-assessment it is likely that the court would encounter situations when the vendor himself meant that he uttered a direction of commercial or professional activities to the Member State of the consumer's domicile while the consumer, at the time of the conclusion of the contract, neither understood the information value of the vendor's utterance to be a direction of such activities nor the reason for which the vendor uttered the information (or vice versa). This is likely to occur when information is uttered through the Internet since the vendor may use another language than the consumer's first language, the structural presentation may be different than what the consumer is used to etc.

It follows that the determination of jurisdiction *ratione loci* cannot be based according to the second alternative alone. This is substantiated by the fact that the wording of Art 15.1c) does not require that the commercial and professional activities must be directed to a consumer in his State of domicile, but rather that these activities must be directed ¨to the Member State of the consumer's domicile¨, which refutes that the court can determine the consumer's understanding of whether activities have been directed and the quality of such activities. Accordingly, if the court were to determine jurisdiction *ratione loci* according to an understanding of whether there has been a relevant direction of certain qualitative activities, the court would have to construe a collective understanding for the Member State as such, which seems rather ridiculous.

Further, it follows that a combination of the two alternatives is a complicated two-step assessment for the court to delimit and localize the legal relationship in the sphere of a jurisdiction and to determine the attribution of competence to court to adjudicate the subject according to a unitary application of the jurisdictional rules, while the disputing parties would experience difficulties in establishing a highly predictable rule.

Finally I would like to point out that in relation to the first alternative that the parties as well as the court may have difficulties in evidencing what activities were carried out on the vendor's website, if these activities were ¨commercial or professional¨, whether there has been a direction of such activities since such activities over time often are changed in form and function.

In the following sections, it will be discussed, without giving a clear answer, which alternative that should prevail.

4. Can an inaccessible website in the Member State of the consumer's domicile constitute a direction to that Member State?

Presupposing that the vendor only directs his activities through the Internet and via a website by making the website accessible for consumers from State A and B, but not from the consumer-plaintiff's Member State C, the question arise whether the expression in Art 15.1c) ¨by any means, directs … to¨ requires that the website directing the ¨commercial or professional activities¨ is accessible in the Member State C of the consumer's domicile in order for Art 15.1c) to apply *ratione loci*.

The European Parliament proposed to clarify the expression "directs such activities" and substitute the Commissions recital 13 when stating in its' Amendment 36 that "[…] electronic commerce in goods and services by means *accessible* in another Member State constitutes an activity directed to that State […]¨ (emphasis added).[39] Even though the Commission rejected the Parliament's amendment in full, the statement makes sense since it is difficult to argue that an inaccessible and invisible website not displaying commercial or professional activities directs such activities to the Member State.

However, it must be stressed that even though this article is concerned with direction of commercial and professional activities through websites, it must observed that accessibility to a website is not a requirement for direction since the channels representing such activities must be considered cumulatively (see Chapter II, point 1).

5. Can knowledge of an accessible website in the Member State of the consumer's domicile in itself constitute a direction to that Member State?

On this point the Commission stated in its initial proposal that "[t]he fact that a consumer simply had *knowledge* of a service or possibility of buying goods via a passive website accessible in his country of domicile *will not trigger the protective jurisdiction*",[40] (emphasis added). The Commission's semantics are unclear referring specifically to "passive" websites. However, it makes no sense to distinct "passive" from "active" websites when assessing knowledge alone as a criterion. This understanding is further substantiated in

---

39 See Amendment 36 of the EP opinion 1st reading, supra note 19.

40 See the Commission's initial Proposal for a Council Regulation, supra note 17.

the proposed recital (13) where the Commission states that the "goods or services by a means accessible in another Member State constitutes an activity directed to that State" as well as the wording of the final act. Thus, according to the Commission, it seems clear that the customer's mere knowledge of an accessible website in itself is insufficient to ground jurisdiction.

6. Can the conclusion of the contract in itself constitute a direction to the Member State of the consumer's domicile?

According to the Brussels Convention Art 13, paragraph 3, point (a) and (b) the right of a customer or vendor to bring an action was intimately linked to the contract concluded between the parties inasmuch as there was an in dissociable relationship established between the vendor's invitation or advertisement in the Member State of the consumer's domicile containing the offer and the customer's order while physically[41] being in the State wherein the invitation and advertising was received, which granted the consumer the right to sue or be sued in that State. The Brussels I Regulation alters and corrects this construction to the contrary and is not concerned with wherefrom the consumer took the steps necessary and wherefrom the contract was concluded in order to apply *ratione loci*. The place where the consumer takes these steps may be in many States and difficult or impossible to determine, both on-line and off-line. Also, this criterion was considered irrelevant for creating a link between the contract and the consumer's State.[42] Thus, the amendment in the Brussels I Regulation Art 15.1c) removes a proved deficiency in the Brussels Convention Art 13, namely that the consumer could not rely on this protective jurisdiction when he had been induced, at the co-contractor's instigation, to leave his home State to conclude the contract.[43]

The wording of Art 15.1c) requires however that a contract must be concluded. This raises the question whether the consumer's entry into contract *in itself* can constitute a direction to the Member State of the consumer's domicile. In its amended proposal, where the Commission rejected the Parliament's proposal in full, the Commission stated that "Moreover, the existence of a consumer dispute requiring court action *presupposes* a consumer contract. Yet the very *existence of* such *a contract* would seem to be a *clear indication* that the supplier of the goods or services *has directed* his activities towards the state

41 See *Foss, Morten and Bygrave, Lee*, p. 124-25, supra note 9.

42 See the Commission's initial Proposal for a Council Regulation, supra note 17.

43 See the Commission's initial Proposal for a Council Regulation, supra note 17.

where the consumer is domiciled",[44] (emphasis added). Some scholars have discussed whether this statement is an argument in favour for establishing a rule where after it is sufficient to ground jurisdiction on the basis of the entry into contract in itself.[45] Others have argued that if there exists a contract, the vendor's activities must be considered as having been directed towards a Member State unless he can prove otherwise. However, the statement, in particular the wording "existence of a contract […] clear indication […] has directed" should be considered as nothing more than a sign of such direction, however whether the vendor's activities have been directed towards the Member State must be separately assessed otherwise the term would be redundant, run counter to its function to provide the sufficient, necessary and determinative link for asserting jurisdiction, and granting the vendor his right to some predictability as to determine where he can sue or be sued pursuant to contracts concluded within the scope of where his activities are directed to, and not by the mere entry into and existence of a contract.[46] Thus, it seems clear that the mere entry into a contract between a consumer and the vendor in itself is insufficient to ground jurisdiction. The unclear point is what suffices of something more than actual knowledge of an accessible website and the mere entry into a contract to ground jurisdiction. The preparatory reports are unclear. A number of assessment factors will be discussed below.

7. Can factual access of a website without any more constitute a direction to the Member State of the consumer's domicile?

The preparatory reports are ambiguous on this point. The Commission stated in its initial proposal that "[t]he concept of activities pursued in or directed towards a Member State is designed to make clear that point (3) *applies to consumer contracts concluded via* an interactive website *accessible in* the State of the consumer's domicile", and further that "[t]he contract is thereby treated in the same way as a contract concluded by telephone, fax and the like, and activates the grounds of jurisdiction provided for by Article 16" (emphasis added).[47]

First, the expression in the preparatory works suggests that, in order to enjoy the protection of Art 15.1c), the consumer must do something more than factually accessing the website, without any more, and that the con-

---

44 See paragraph 2.2.2 of the Commission's amended Proposal for a Council Regulation, supra note 18.

45 See *Diana Wallis*, the Rapporteur of the European Parliament, Amendment 23, supra note 2.

46 See *Øren, S. T., Joakim*, p.680, supra note 27.

47 See the Commission's initial Proposal for a Council Regulation, supra note 17.

sumer must engage in contractual activities such as the negotiation or the conclusion of a contract to purchase goods or services.

Second, Art 15.1c) does not require that the contract has been concluded from the State of the consumer's domicile via an interactive website accessible in the State of the consumer's domicile, but rather that the contract has been concluded between a consumer, whose location when concluding the contract is irrelevant, with a vendor who, by any means, directs such activities to the Member State of the consumer's domicile or to several States including that Member State. In other words this means that the consumer in practice can conclude the contract from anywhere and still enjoy the protection of Art 15.1c) provided that the commercial or professional activity has been directed to the Member State of the consumer's domicile or to several States including that Member State. This is substantiated by the fact that a consumer could access a website from anywhere, and unless the competent forum was the Member State of the consumer's domicile, the consumer dispute could very easily be attributed to courts in all the Member States.

Further, the question arise whether the preposition "concluded via" means that the contract directly must be concluded digitally through the website's employment of communication-services to communicate that the obligation freely has been assumed by one party towards another, or whether the contract also can be concluded through some other mean of communication such as telephone or fax. As mentioned, the wording of Art 15.1c) does not operate with any requirement as to the medium to communicate and agree on a contract. Moreover, such a criterion would run counter to the philosophy of Art 15 which is to afford the consumer better protection. Thus, it seems not be in accordance with Article 15.1.c) that the contract directly must be concluded digitally through the website's employment of communication-services to communicate that the obligation freely has been assumed by one party towards another. Rather, it is the author's view that there is no requirement as to what medium the contract as been concluded through.

8. Must the conclusion of the contract have been preceded by a direction of commercial or professional activities to the Member State of the consumer's domicile?

In comparison with the Brussels Convention Art 13, paragraph 3, point (a) where it was required that ¨[…] the conclusion of the contract was preceded by a specific invitation addressed to [the consumer] or by advertising¨, the text of the Brussels I Regulation Art 15.1c) merely provides that ¨[…] the contract has been concluded with a person who [by any means, directs] commercial or professional activities [to] the Member State of the consumer's

domicile or to several States including that Member State […]¨. Thus, it seems not relevant, in order to ground jurisdiction *ratione loci*, that the conclusion of the contract must have been preceded by a direction of commercial or professional activities to the Member State of the consumer's domicile or to several States including that Member State.

However, it must be observed that Art 15.1c) requires that the contract, which has been concluded, must fall ¨[…] within the scope of [the directed commercial or professional] activities¨ to the Member State of the consumer's domicile.[48]

If this was the intention, Art 15.1c) forces the vendor to continuously be clear as to where he directs his activities, since contracts entered into not only after, but also before the direction of commercial and professional activities, will suffice to ground jurisdiction. If this is the correct understanding, the consumer is granted a far better protection than in the Brussels Convention Art 13, paragraph 3.

9. Does the expression ¨directs commercial or professional activities to the Member State of the consumer's domicile¨ require a quantitative direction to that Member State?

This question can be separated in two. First, does the said expression require direction to the Member State of the consumer's domicile as such, or can a website, which is for example inaccessible in the Member State of the consumer's domicile, yet accessible therein for one consumer who concludes the contract, constitute a direction to that Member State?

It must be observed that the wording of the Brussels I Regulation requires that the activities must be directed ¨ *to* [the] Member State [of the consumer's domicile] or to several States including that Member State¨ (emphasis added). This indicates that the activities must be directed to the Member State as such, and that it is insufficient to ground jurisdiction if such activities were directed to one (specific) consumer as by contrast was sufficient in relation to the Brussels Convention Art 13, first paragraph, point (a), where after a specific invitation must have been addressed to the consumer or by advertising in the State of the consumer's domicile. On this point the preparatory works are imprecise when they merely state that the philosophy of the new Article 15.1c) is that the co-contractor creates the necessary link when directing his

[48] This special condition was designed to establish a close connecting factor between the dispute and the court, and to ensure that there are close connections between the contract in issue and the State in which the consumer is domiciled.

activities towards the consumer's State.[49] However, since the intention of Art 15.1c) was to grant the consumer a better protection than its predecessor, it should be plausible to argue that Art 15.1c) applies even if the activities were directed only to one consumer.

Second, does the said expression require a quantitative direction of the qualitative criterion "commercial and professional activities" in order for Art 15.1c) to apply *ratione loci*?[50]

The wording operates with the plural form "activities". This seems to be a deliberate choice since the nouns "commercial activities" and "professional activities" are not preceded by a singular form as in ¨a commercial or professional activity. This indicates that Art 15.1c) requires a quantitative direction of the qualitative criterion "commercial and professional activities" in order for Art 15.1c) to apply *ratione loci*.

This interpretation was supported by the European Parliament who proposed to clarify the expression "directs such activities" and substitute the Commissions recital 13 when stating in its' Amendment 36 that "[…] electronic commerce in goods and services by means accessible in another Member State constitutes an activity directed to that State where the online trading site is an active site in the sense that the trader purposefully directs his activity in a *substantial* way to that other State" (emphasis added). This interpretation was substantiated in Amendment 37 where the Parliament stated that "[t]he expression "directing such activities" shall be taken to mean that the trader must have purposefully directed his activities in a *substantial* way to that other Member State or to several countries including that Member State" (emphasis added).[51] The Parliament meant, without commenting on what activities that constitute a "substantial direction", that only such direction could trigger the protective consumer jurisdiction.

On the other hand, the Commission could not accept the Parliament's proposal relating to Art 15. In its' reasoning, the Commission did not pinpoint what it exactly rejected as it reasoned in general terms. The Commission's statement that the "Parliament proposes a new paragraph to define the

---

[49] However, in order for Art 15.1.c) to apply it is required that the contract concluded between the consumer and the vendor must fall within the scope of the commercial and professional activities pursued in or directed to the Member State where the consumer is domiciled.

[50] The term "commercial and professional" is a qualitative criterion defining which of the vendor's activities that are relevant. This term is wide in scope, and includes all of the vendor's activities cumulatively regardless of mean of direction, whether it is by the general press, radio, Television, Internet etc. Finally, the term "activities" is by wording a quantitative criterion by the plural form "activities".

[51] See Amendment 36 of the EP opinion 1st reading, supra note 19.

concept of activities directed towards one or more Member States, and takes as one of its assessment criteria for the existence of such an activity any attempt by an operator to confine its business to transactions with consumers domiciled in certain Member States" (emphasis added) seems to presuppose that the Commission's perception of the Parliament's proposal did not operate with a criterion referring to some quantity of direction, which the Parliament exactly did. It follows that the Commission's statement on this point should not be taken as a rejection of this specific point in the Parliament's proposal.

Further, the Commission stated that the Parliament's "[…] definition is based on the essentially American concept of business activity as a general connecting factor determining jurisdiction, whereas that concept is quite foreign to the approach taken by the Regulation." This statement refers presumably to the minimum contacts test under the Due Process analysis to the US Constitution where the jurisdictional principles regarding "general jurisdiction" requires a "systematic and continuous contact" while the contacts sufficient for "specific jurisdiction" may be a single or isolated contact[52] (the quantitative requirement) as long as the contact is not random. This statement may be understood in such a way that there is no requirement as to substantiality in direction of the commercial or professional activity.

Moreover, regarding the Brussels Convention Article 13, first paragraph, point 3(a), in circumstances, where a consumer has been contacted by personalized letters at his home sent by a professional vendor for the purpose of bringing about the placement of an order for goods offered under the conditions determined by that vendor, the ECJ has ruled in *Rudolf Gabriel* that one or more letters are sufficient to fulfill the condition in Article 13, first paragraph, point 3(a) "in the State of the consumer's domicile the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising" provided that the consumer has in fact placed such an order in the Contracting State in which he is domiciled.[53] It is unclear to what extent this judgment is of guidance as to jurisdiction pursuant to the new Art 15.1c), and the question arise whether the expression "one or more letters" applies by analogy to Art 15.1c). On the one hand, the judgment's formulation is specific to circumstances of the case "[i]n those circumstances", suggesting that "one or more letters" are sufficient when the letters were personalized and addressed to the consumer. On the other hand, the wording of the Brussels Convention Art 13, first paragraph, point 3(a) is formed in singular "[…] a specific invitation addressed to him or by advertising" indicating that one or more invitations or one advertisement were sufficient to ground jurisdic-

---

[52] See e.g. *McGee v. international Life Insurance Co.*, 355 US 220 (1957), where a single insurance contract was sufficient.

[53] *Rudolf Gabriel*, Case C-96/00, European Court Reports 2002 p 6367, paragraphs 52 and 53.

tion. Since the aim of Art 15.1c) second alternative is to improve the protection of the consumer in relation to its' predecessor Art 13 of the Brussels Convention, it should be plausible to argue that there is no requirement as to substantial direction in order to ground jurisdiction.

It is unclear how the general jurisdictional objective, that the designation of forum must establish a rule of jurisdiction that is highly predictable, is to be applied. This objective does not only favor the reasonableness for the well-informed defendant to foresee where he can be sued, but also for the well-informed plaintiff who easily should be able to identify the competent forum. It may be easier to identify the place where to commercial or professional activities have been directed by operating with a criterion requiring any and even one direction than operating with a certain minimum of direction of such activities. When the commercial activities are directed by the vendor to the customer in a specific territory and the customer concluded the contract for the purchase of goods or services essentially, or exclusively, by reason of the vendor's direction of commercial activities involving an offer and a promise of delivery to the customer, it is plausible to argue that both the customer and the vendor can foresee that it is justifiable to bring an action in the country whereto the vendor directed his/her offers regardless of relying on the quantity of the direction.

Moreover, this would enhance and amplify the special objective behind Art 15, which is to ensure adequate protection for the consumer who is considered deemed to be economically weaker and less experienced in legal matters than his professional co-contractor thereby avoiding the burden of assessing whether direction of the commercial activities were sufficiently substantial.

10. Does the expression ¨directs … to the Member State of the consumer's domicile¨ require a purposeful direction to that Member State?

This question is relevant in many respects. Taking the example of websites[54], even though commercial or professional activities are carried out through a

[54] Particular problems arise when the activity by e-mail is directed to the consumer without prior action from the consumer. How shall such an express offer be characterised regarding purposefulness? If the e-mail address does not indicate the consumer's domicile, it is more problematic to argue that the activities are directed to the Member State of the consumer's domicile than if the e-mail address end s with e.g. .de for Germany. Also, if the consumer is domiciled in another State than what the e-mail address indicates in the end of the domain name, e.g. a Greek consumer has an e-mail address ending with .de, the question arise whether jurisdiction *ratione loci* in Art 15.1.c) allocates jurisdiction to adjudicate the dispute in Greece? Would it make a difference if the Greek consumer gives the vendor the impression that he is domiciled in Germany (see Capter II, point 9)?

website, the vendor may not purposefully direct his activities to one or more specific Member States. This is clearly demonstrated when a website is inaccessible in State Y or when the website only conducts commercial and professional activities with State X. If in such circumstances, when the activities, neither factually nor purposefully, are directed to State Y, the vendor makes a purposeful exception and enters into a contract with a consumer who is domiciled in and concludes the contract from State Y, the question arises whether this direction of activity grounds jurisdiction *ratione loci* since there was a purposeful direction of activities. Also, presupposing that the meaning of the expression ¨by any means, directs … to¨ does not include what has been done to avoid directing commercial and professional activities towards one or more specific Member States (see point 9 below), while the vendor still employed reasonable measures not to direct commercial and professional activities to the Member State of a consumer's domicile, but by accident entered into contract with a consumer in that Member State, it is questionable whether the vendor's entry into contract with the consumer does not constitute a direction to that State since it was not purposeful.

Whether the direction of activities to a Member State was purposeful may be evidenced either by subjective evidence or evidence based on an objective assessment of which, how (and through what channel of communication) the commercial and professional activities have been employed in direction to a Member State (imputed intentions)). Thus, the wording ¨directs¨ suggests that in order for Art 15.1c) to apply *ratione loci*, there must be more than a website that is accessible in the Member State and represents digital signs signifying commercial and professional activities.

In relation to the Brussels I Regulation the Parliament[55] proposed in its amendment 36 and 37 respectively that "[i]n particular, electronic commerce in goods and services by means accessible in another Member State constitutes an activity directed to that State where the on-line trading site is an active site in the sense that the trader *purposefully* directs his activity in a substantial way to that other State.", and that "[t]he expression "directing such activities" shall be taken to mean that the trader must have *purposefully* directed his activities in a substantial way to that other Member State or to several countries including that Member State", (emphasis added).[56] The Commission stated that the Parliament's "[…] definition is based on the essentially American concept of business activity as a general connecting factor determining jurisdiction, whereas that concept is quite foreign to the ap-

[55] See also the Opinion of the Economic and Social Committee who stated that "[t]he question is whether promoting its services on the Internet means that a company is *deliberately* seeking to expand beyond its traditional marketing area¨ (emphasis added), supra note 2.

[56] See Amendment 36 of the EP opinion 1st reading, supra note 19.

proach taken by the Regulation." As already indicated, this statement refers presumably to the minimum contacts test under the Due Process analysis in the US Constitution where the jurisdictional principles regarding purposefulness and "specific jurisdiction" under the concept of minimum contacts requires that the defendant purposefully avails himself of some benefit of conducting activities within the forum-state, thus invoking the benefits and protection of its laws and implying that the requirement of purposefulness is not fulfilled if the defendant has had no contact with the forum.[57] This statement may be understood in such a way that there is no requirement as to purposefulness in direction of the commercial or professional activity to a Member State.

Also, the view of the Parliament has been criticised on the basis that it is difficult to determine what the substantive content is when operating a website and further what assessment factors to employ to determine whether or not the vendor had a subjective meaning regarding whereto he directed his commercial activities.[58]

On this background it should be plausible to conclude that there is no requirement to ground jurisdiction that a vendor directs his commercial and professional activities to a Member State on subjective intentions.

However, it seems clear, in accordance with the philosophy behind Art 15.1.c) that the co-contractor creates the necessary link when directing his activities towards the Member State, that this direction must be evidence based on an objective assessment of which and how (see point 9 b) below) the commercial and professional activities have been employed in direction to a Member State (imputed intentions) where after the vendor's and consumer's expectations as to where they can sue or be sued must have reference to this activity and not the mere conclusion of a contract.

---

[57] Regarding purposefulness and "*general jurisdiction*" the contact between the defendant and the forum must also here be the result of the defendant's own purposeful action, regardless of whether or not the defendant is engaged in "systematic and continuous" activities within the forum. However, it is rather unthinkable that "systematic and continuous activities" in a state can be conducted without purpose.

[58] Regarding the Brussels I Regulation Art. 15.1c), see *Øren, S. T., Joakim*, p. 686-87, supra note 27. Regarding the Brussels Convention Art. 13, paragraph 3, see *Foss, Morten and Bygrave, Lee*, p. 118, supra note 9, where the authors comment on the Guiliano-Lagarde Report.

11. Does the expression ¨directs … to¨ require an active direction or avoidance of direction, or both an active and avoidance of direction of commercial or professional activities to the Member State of the consumer's domicile¨?

When interpreting the expression "directs … to", three main methods are distinguishable.

The first is concerned with a positive definition of the Member States to which the vendor actively directs his commercial and professional activities. The second is concerned with a negative definition of the Member States, and focuses on what has been done to avoid directing commercial and professional activities towards one or more specific countries by ring-fencing the vendor's trading operation against transactions with consumers domiciled in particular Member States.[59] The third is a combination of the first two.

These distinctions are rather a sliding scale of degrees of active direction or avoidance of direction (with degrees of passivity in between) than a clear border.[60]

---

[59] See *Diana Wallis*, the Rapporteur of the European Parliament, p. 35, supra note 2, who presupposes that the Brussels I Regulation is inapplicable where the vendor specifies that his services are not available to consumers resident in the Member State in question. However, the Parliament proposed to clarify the expression "directs such activities" and substitute the Commissions recital 13 stating that "The expression "directing such activities" shall be taken to mean that the trader must have […] directed his activities in a substantial way to that other Member State or to several countries including that Member State. *In determining whether a trader has directed his activities in such a way, the courts shall have regard to all the circumstances of the case, including any attempts by the trader to ring-fence his trading operation against transactions with consumers domiciled in particular Member States*" (emphasis added), see Amendment 37 in the Proposal from the Parliament, supra note 19.
The Commission rejected the proposed amendment by the Parliament. However, this rejection did not refer to the ring-fencing technique, but the concept of purposefulness.

[60] The sliding scale test originated from U.S. case-law, first in the *Zippo Mfg. Co. v. Zippo Dot Com, Inc.* 952 F. Supp. 1119, (W.D. pa. 1997), see supra note 21. In order to constitutionally exercise personal jurisdiction since such exercise was directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. The court addressed the spectrum of how a defendant may conduct business over the Internet and introduced the sliding scale test where after adjudicative jurisdiction normally was seized if the website was classified as "*active*" referring to websites where the website operator enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmissions of computer files over the Internet, while normally dismissed if the website was "*passive*" referring to situations where a defendant has simply posted information on an Internet Web site, which is accessible to users in foreign jurisdictions. A third classification was "*interactive*" websites where a user can exchange information with the host computer and where after courts can seize adjudicative jurisdiction depending on the level of interactivity and commercial nature of the exchange of information that occurs on the Web site (see 952 F. Supp. 1119, (W.D. pa. 1997), p. 1124.). Later this test became a precedent for other U.S. courts to

Noteworthy in an e-commerce context are the difficulties deciding what constitutes a direction or avoidance of direction of commercial or professional activities to a Member State. Under which category falls e.g. a statement from a German vendor that 1) "consumers domiciled in Greece are not allowed to purchase this software-program" (done to avoid directing activities towards a specific country), 2) ¨this software-program can only be purchased by consumers domiciled in Greece¨ (done actively to direct activities towards a specific country), 3) ¨this software-program can only be purchased by consumers domiciled in Greece and not by consumers domiciled in any other State¨ (done actively to direct activities towards a specific country, while the second focuses on what has been done to avoid directing activities towards a specific country).

Thus, two discussions are necessary. First, one must for the purpose of jurisdiction define the country specific elements of the vendor's commercial and professional activities regardless of whether or not the term "directs" means either or both a positive direction to or negative avoidance of direction to.

Second, if the term "directs" means either a positive direction to or negative avoidance of direction to, one must, for the purpose of jurisdiction, consider the relevance and weight of the country specific elements of the vendor's commercial and professional activities as allowing or disallowing transactions with consumers in specific Member States.

a) Active direction to, avoidance of direction to, or a combination of such direction to specified Member States?

The Parliament supported both methods in its proposition where it sought to define the Commission's suggested criterion in recital 13 "activity directed to that State" stating that "[i]n determining whether a trader has directed his activities in such a way, the courts shall have regard to all the circumstances of the case, including any attempts by the trader to *ring-fence* his trading operation against transactions with consumers domiciled in particular Member States", (emphasis added).[61]

Further, the Rapporteur for the Committee on Legal Affairs and the Internal MarketDiana Wallis, confirmed that "[b]esides, it is always open to the en-

---

follow as well as Canadian courts (see e.g. *Braintech Inc. v. Kostituk*, [1999] 171 D.L.R. (4th) 46, 61 (B.C.C.A.) (defamation). The Zippo-test showed many inconsistencies, and was difficult to practice, thus U.S. courts expressed that "something more" than mere web presence must justify adjudicative jurisdiction, and this "something more" must show that the defendant directed the content towards the forum state, see e.g. *Cybersell Inc. v. Cybersell, Inc.* 130 F.3d. 414 (9th Cir. 1997) (infringing service mark)).

61 See EP opinion 1st reading, supra note 19.

trepreneur to specify that his services are not available to consumers resident in certain Member States and in this way to avoid concluding contracts outside his own Member State."[62]

When reconciling the three above stated objectives of the Brussels I Regulation in relation to e-commerce – namely to serve, promote and cultivate the growth of e-commerce in the EU, to ensure persons domiciled therein not to be deterred from using the Internet to promote their goods and services in order to support competitiveness of European companies at global level, and to guarantee the best possible legal protection for its citizens, and especially consumers, in relation to the development of e-commerce and its risks - it can be argued that the rejection of the second alternative as a determinative criterion for asserting jurisdiction would negate the two first objectives. Rather than to serve, promote and cultivate the growth of e-commerce in Europe and at a global level, the result could be that Art 15.1c) would impede the continued development of e-commerce because businesses would not[63] go on-line, stop or limit their use of the Internet as a channel for commerce due to the fear of being hauled into courts in jurisdictions where they do not want to direct their business activities. There is in fact a danger that the prospect of having to deal with litigation in any Member State might be perceived as outweighing the attractions of Internet trading. This can potentially lead to a less efficient market in the EU either directly or indirectly, factually or potentially, and can therefore hinder the maintenance and development of an area of freedom, security and justice. Also, the EU may on a global level loose the chance of providing a lead in this new market whose possibilities appear virtually limitless.

Further, it can be argued that predictability so as to avoid directing commercial and professional activities to specified Member States hence avoid being haled into court is a fair criterion since it counterbalances the abandonment of predictability in the Brussels Convention Art 13, paragraph 3, where after the conclusion of the contract from the Member State of the consumer's domicile whereto the invitation was sent was determinative for jurisdiction.

On the other hand, a natural understanding of the wording "directs" suggests that the Brussels I Regulation has taken the view that the determinative criterion for allocation of jurisdiction to court is the vendor's active direction of commercial or professional activities towards a Member State and not the vendor's activities of avoiding such direction.

---

62 See Diana Wallis, the Rapporteur of the European Parliament, p. 35, supra note 2.

63 Small and medium-sized businesses in particular may be dissuaded from making the investment needed in order to open Internet sites unless ring-fencing their trading operations is determinative for the allocation of jurisdiction to court.

This is supported by the Commission who rejected this view in its' amended proposal stating that the "Parliament proposes a new paragraph to define the concept of activities directed towards one or more Member States, and takes as one of its assessment criteria for the existence of such an activity any attempt by an operator to confine its business to transactions with consumers domiciled in certain Member States. The Commission cannot accept this amendment, which runs counter to the philosophy of the provision."[64] If a vendor has ring-fenced his trading operation as far as possible with a particular Member State, and a consumer in that Member State still is able to conclude a contract with the vendor through his website, it would negate the policy to prioritise the consumer and grant him the right to sue or be sued in the Member State of his domicile. To compel consumers to sue in foreign courts would be disproportionate and unreasonable in view of the low value of most consumer Internet transactions, the teething troubles of the infant Internet trading industry[65] and the cost and inconvenience of bringing proceedings abroad.

Moreover, the necessity for consumers to sue in a foreign court might itself prove a strong deterrent to Internet trading. From an e-commerce perspective, the consumer's disadvantage (and conversely the vendor's advantage) is often to be deprived from negotiating the terms of the contract and to be obliged to pay in advance by credit card before the object of the contract is performed. If a dispute arises, the practical and economical effect of Art 15.1c) is that the vendor must sue or be sued in the Member State of the consumer's domicile and often cover the extra costs associated with court litigation in a foreign State. This is in a way fair since the vendor, who reaches a global marketplace through the Internet, potentially leading to increased transactions and revenues, can insure himself against such expenses and incorporate the insurance costs etc in sales prices and demand tax reductions.[66]

Furthermore, the Commission emphasized in its' amended proposal when rejecting the Parliament's ring-fencing consideration, that "[l]astly, this definition is not desirable as it would generate fresh fragmentation of the market within the European Community."[67] If the criterion "by any means directs … to" is to be understood as also including attempts by the trader to ring-fence his trading operation against transactions with consumers domiciled in particular Member States, the effect would be that many vendors would avoid

---

64 See paragraph 2.2.2 of the Commission's Amended proposal, supra note 18.

65 *Ernst & Young*, the management consultancy, estimated that one in six goods bought by US online shoppers last Christmas never arrived.

66 See *Diana Wallis*, the Rapporteur of the European Parliament, p. 10, supra note 2. See also note 32.

67 See paragraph 2.2.2 of the Commission's Amended proposal, supra note 18.

transactions with consumers in certain Member States in order to hinder being haled into court in jurisdictions favouring consumer rights. For mere jurisdictional purposes, such a rule would in fact allow the vendor to choose the court(s) (forum-shopping), which the Brussels I Regulation as far as possible seeks to avoid. The Commission's statement reflects the purpose of the Brussels I Regulation that it must be applied and interpreted in a way which is compatible with Community law and in particular neither hinders nor makes less attractive the exercise of the fundamental principles of free movement of goods and services guaranteed by the Treaty and Directives concerning the application of these principles in certain areas. Considering the intra-community legal order as a whole, it would be a paradox if the jurisdictional rules gave a clear incentive for vendors to employ technical and legal measures to exclude and discriminate consumers in some jurisdictions from concluding contracts, and also to utilise technology to identify who the potential customer is and wherefrom[68] he interacts with a website thereby increasing the cross-border flow and use of privacy information counter to data protection legislation[69]. Also, it would be a paradox if such a criterion would lead to the same effects as various methods of protectionism and trade barriers as well as discrimination by not treating consumers equally. This is counter to liberal trade policies, based on the statistical link between freer trade and economic growth, supported by economic theory (the principle of comparative advantage) and the experience of open, fair, sharp and undistorted competition, which motivate innovation, efficiency among producers to provide up to date and attractive goods and services to consumers and multiply the rewards that result from producing the best products with the best design at the best price at the place with the lowest cost and offering the products to other markets. Accordingly, the damage caused by such a criterion would lead to unfair trade, discrimination and a self-defeating and destructive drift into protectionism. Unless this paradox in structural terms was solved by differentiation in hierarchical legislation, or a harmonisation on the same hierarchical level of legislation, this could in several respects create a situation of irreconcilable situations for vendors who would be forced to choose which legislation(s) to follow, and which to breach by foster a climate for breaching of Community law and increase the workload for courts that would also be facing the problems of giving irreconcilable judgments. On this point, a directing-test should have a

---

[68] Such technical assessment factors presuppose and include an assessment of whether or not the vendor has received and been aware of information sent from the consumer.

[69] See the Directive 95/46/EC of the European Parliament and of the Council of 24 Oct 1995 on the protection of individuals with regard to the processing of personal data and of the free movement of such data, OJ L 281, 23/11/1995, 31.

uniform substantive content allied to the European Community legal order since it is indispensable for the coherence of its provisions.

Additionally, if the criterion "by any means directs … to" is to be understood as also including attempts by the trader to ring-fence his trading operation against transactions with consumers domiciled in particular Member States, the techniques employed to avoid such transactions would not always factually hinder a contract to be concluded (e.g. a statement from the vendor specifying that customers in Germany are not allowed to conclude contracts which can be performed digitally through the Internet), and if so, Art 15.1c) would be inapplicable by way of criteria that are not transparent to the consumer, and thus neither granting the consumer the protective right he should enjoy by Art 15.1c) nor a highly predictable rule, whether the consumer is a plaintiff or a defendant.

Thus, on the basis of the preparatory works and the objectives proper for Section 4, it should be plausible to conclude that the expression "directs" is a criterion that refers to the vendor's active direction of commercial or professional activities to be available to consumers in particular Member States and not that they are unavailable.

If at all ring-fencing should be determinative, it should be discussed what elements that should be relevant/irrelevant. This is a long discussion, which the author will not comment on in detail here. It is sufficient to say that for the justification of allocation of jurisdiction to court, the relevant elements of ring-fencing should be subject to strict transparency requirements which avoid any risk of inadvertence and uncertainty as to jurisdiction.[70]

Lastly, it must be questioned whether it is justified to invoke the applicability of Art 15.1c) if the consumer misleads the vendor to believe that he is for example domiciled in Germany, but in fact is domiciled in Greece, or if the customer declares himself as acting in the course of business?[71] Provided that the vendor is in good faith as to where the consumer is domiciled[72] or in what capacity the customer acts, it can be argued that the application of the

---

[70] Another side of the ring-fencing technique is of course to employ technical measures, which do not allow consumers to conclude a contract from specified Member States. However, it must be borne in mind that even if the vendor employs such procedures, he may be sued in one of those Member States provided that the court determines that the vendor by any means has directed its commercial and professional activities to the Member State in question.

[71] This problem can arise when e.g. the vendor employs self-registration procedures. Regarding similar problems on the side of the vendor, see point 8.

[72] Good faith is more likely to be present when the object of the contract is performed by transmission through the Internet compared to performance by ordinary mail where the vendor must send the object of the contract to the address the vendor states, which normally will be the place where the consumer is domiciled.

rules of special jurisdiction laid down in Art 15.1.c) should not be extended to persons for whom that protection is not justified, and that these two situations do not justify its application.[73]

b) What assessment factors should be relevant pursuant to the scope of application jurisdiction ratione loci "by any means, directs … to"?

At this point in time there exist no standardized and functional technical solution for identifying geographical customer relations and thereby localize, by technological measures, the legal relationship within the sphere of one or several predetermined jurisdictions. Hence, the interplay between the vendor's trading operation and the customer forms the parties' expectations, particularly on the part of the customer, who, before entering into a contract with the vendor, often bases his dispositions on other factors than an agreement. These factors are unilaterally dictated by the vendor, and signalize preconditions for interaction and transaction with the customer, either by personal or automated interaction.

When identifying such factors, one must as mentioned, bear in mind that both on-line as well as off-line activities are relevant, whether related to e-commerce operations or any other activity such as TV, radio, telephone, fax etc.[74] Here, the author will solely look at elements limited to e-commerce carried out by electronic means. Whether or not these elements must be considered cumulatively, depends on which elements that direct the commercial and professional in question.[75] This question will not be commented on here, but it must be observed that direction of commercial or professional activities often consist of a plurality of elements and not one singular act or channel of communication (see Chapter II, point 1).

Relevant country-specific factors includes the concrete Internet services employed for the digital interaction between the vendor and the consumer in addition to other communication- and information services with no limitations. Under this category problems arise whether country specific indicia

---

73 Regarding the Brussels I Regulation, see *Øren, S. T., Joakim*, p. 693, supra note 27. Regarding the Brussels Convention Art 13, paragraph 13, see *Foss, Morten and Bygrave, Lee*, p. 106, supra note 9; *Stone, Peter*, p. 9, supra note 9.

74 It is advisable for vendor's both to clarify as well as emphasize in a transparent way to the consumer what commercial and professional activities that are country-specific and directed to each Member State.

75 Assuming that it is clear that e.g a German vendor employs a website ending on .de to direct his commercial and professional activities to Germany, while he in addition on the website provides a Chat room open for everyone to discuss in English his products, the question arise whether the direction of activities should be considered in relation to the website, the Chat room or both.

such as the distinctions relating to .com, .org, etc vs .no, .de etc should be relevant.

Further, another country-specific factor are the technological features employed by the vendor to conduct country-specific transmissions that either allows or rejects transmissions in order to aim at or avoid specific jurisdictions. Under this category problems arise whether software filters and other technological screening devices should be relevant.

Additional country-specific factors are the employment of user identification typically based on IP address identification, self-identification, and off-line identification. Under this category problems arise whether e.g. use of geographically limited credit cards are relevant.

Moreover, legal notices that permits or prohibits transmissions to specific Member States are also country-specific factors. Under this category problems arise as to whether invalid forum-selection clauses, and clauses not accepted by the receiver as well as self-statements/declarations from the receiver/user should be relevant.

Finally, the character of the content, whether film, photo, music or text, as well as its presentation, language[76], advertising including eventual offers of shipment and conditions as to monetary currency for payment may represent country-specific factors which may be relevant.

12. Consequences of extending the scope of the intra-Community legal order with the directing-test

As mentioned in Chapter I, jurisdiction in consumer contracts for the intra-Community legal order does not, as the Brussels Convention Art 13, paragraph 3[77], concern itself with legal relationships arising out of offers and conclusions of contracts within its territorial scope, but is rather concerned with effects on its territory, regardless where that effect was sent from,[78] meaning that both actions can origin from anywhere in the world and still fall under

---

[76] See *American Bar Association*, Achieving legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created By the Internet.

[77] The Brussels Convention Art. 13, paragraph 3, provides in point (a) that "*in the State* of the consumer's domicile the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising; and" point (b) "the consumer *took in that State* the steps necessary for the conclusion of the contract", (emphasis added).

[78] Assuming that the other party to the contract, the vendor, is not domiciled in a Member State, the question arise whether the vendor's website can constitute "[…] a branch, agency or establishment in one of the Member States […]", and whether a contractual dispute arising out of the operation of his website is a dispute "[…] arising out of the operation of the branch, agency or other establishment […]" according to the Brussels I Regulation Art. 15.2.

the scope of Art 15.1c). Such a law will give lawmakers legislative and jurisdictional power over all information that is generated on the condition that the information can be understood in that country. This amendment represents a considerable extension of where the legal relationship must be confined in order to allocate jurisdiction. The consequences can be formidable of which I will point out three.

First, the effect of such a rule may incite countries outside the EU (and the ETFA) to take some countermeasures. A clearly discernable trend in national and international legislation is that the scopes of application of the relevant provisions focus on the effects of the communication of information within or what has been directed to a specific territory. This may possibly lead to a global fight pursuant to legislative-, adjudicative- and coercive jurisdiction over accepting or rejecting (direction of) digital signs through the Internet and its mediation of our selection of utterances (constituting information) in various forms, numerous functions and with different degrees of interactivity through its communication- and information services.

Second, and as previously pointed out, borders for communication could, even within the same legislative system such as the EU, lead to legislative paradoxes relating to free speech, competition law, discrimination etc, which in several respects could create irreconcilable situations where people would be forced to choose which legislation they should follow and which to breach which in turn would foster a climate for breaching of law and increase the workload for courts that would also would be facing the problem of giving irreconcilable judgments.

Lastly, and finally, a factual effect of such a rule may be that our selection of utterances, which generate information, should be selected with a particular view to all foreign jurisdictions and legislation. However, adapting communication to foreign legislation in the landscape of the global reach of the Internet is so far impossible. This forces people who utter and generate information to create virtual borders where the one who utters something - e.g. on a website - by binary logic generates identities as to acceptance of e.g. people domiciled only in State X but not State Y. It is as though a global territory will be inscribed on a new map and that communication in society will be broken up in virtual codes and must as a result partly lead to incommunicability. This can be considered as a less severe consequence than stopping communication.