HUMAN ERROR

AND

DATA SECURITY

IRIS21

Ahti Saarenpää

UNIVERSITY OF LAPLAND
LAPIN YLIOPISTO

Ahti Saarenpää

Professor Dr emeritus
Institute for Law and Informatics
Faculty of Law, University of Lapland

Docent

Faculty of Law , University of Helsinki

Vice Chair
Data protection Board (-2020), Finland
Member
Finnish Academy of Science and Letters

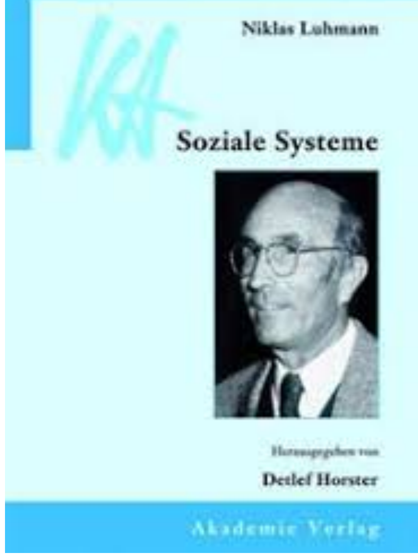
ABSTRACT

To err is human. This is perhaps one thing we can be sure about. And we can make mistakes in the widest variety of situations. Of course, we are quick to apologize, too: we have been taught it is good manners. Yet we readily invoke “human error” as an excuse even when we have made a mistake under rather unique circumstances. In such cases, the legal significance of the error should not be obscured by profuse apologies. **Where IT and information systems are concerned, there is generally little or no tolerance for mistakes**. And human error should have no real place in explaining why an information system fails, nor should it be possible for an error-prone human to use an important system incorrectly. Errare humanum est, perseverare autem diabolicum.

Human error

- Making a mistake is – in theory – a straightforward phenomenon. At the simplest we can speak of an error when something has not gone as we intended or assumed it would. Basically, it is an individual who makes mistakes; we make mistakes. The expression “human error” generally adds the possibility of being forgiven. When we speak of “human” error, we often do so to forestall any serious attempts to determine who or what to blame. The error is “only human”. It could happen to anyone.
- We are also accustomed to talking about forgiveness in ethical and religious contexts. **Apologies are offered and forgiveness given.**

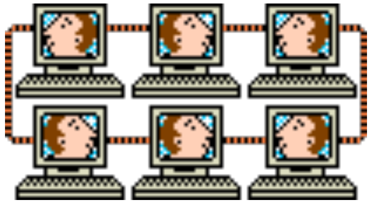
Niklas Luhmann



- One significant distinction *Niklas Luhmann* has offered in his extensive legal and sociological works plays a crucial role here. It is the distinction between *trust* and *trustworthiness*. In somewhat simplified terms, in his system theoretical analysis Luhmann posits that trust is a central element in the actions of a person as a social being. Through trust we reduce uncertainties stemming from the complexity of the world we live in. This is not confined to trust between individuals, which traditionally has played a key role in assessing the validity of legal acts between people.

Network Society – Trust?

- We have advanced from the Information Society to the Network Society or Digital Network Society and Cyber Society. It is a new era in our societal development. It is a society in which the environment we live and work in is shaped to a crucial extent by the use of information systems, databases, collections of data, and information networks. This reliance is markedly different from the increased use of databanks and computers that marked the Information Society. This transformation has also been already observed to some extent at least in **the digital strategy of the EU**.



THL Finland

Finnish institute for
health and welfare

- The Finnish Institute for Health and Welfare (THL), as a government institution, maintains a signifi-cant number of registers with data on health and illnesses. In essence, the information they contain is confidential. Nevertheless, the personal data of some 6,000 persons in the laboratory system were on the open Internet and accessible to search engines from 29 January 2017 to 17 August 2018. The basic reason was that in 2015 the data had been saved as an object rather than as an image. Accordingly, the background information was linked to a slide on the web page. In January 2016 the slideshow was placed on Institute's public network and – to top it all off – in April was uploaded to the Institute's external, public docshare service. It remains unclear who uploaded it. A member of the public noticed the data and reported the case to the Finnish Data Protection Ombudsman.   The Institute then stated **that the lapse was a case of human error**.

GIG CYMRU NHS WALES Iechyd Cyhoeddus Cymru Public Health Wales

Wales

We can see a somewhat similar case in Wales at the end of August 2020. Public Health Wales reported that the personal data of 18,105 persons who had been tested for the Covid-19 virus and had tested positive were available on a public server. In reporting the case, Public Health Wales stated the following: “The incident, which was the result of individual human error, occurred on the after-noon of 30 August 2020 when the personal data of 18,105 Welsh residents who have tested positive for COVID-19 was uploaded by mistake to a public server where it was searchable by anyone using the site. After being alerted to the breach we removed the data on the morning of 31 August. In the 20 hours it was online it had been viewed 56 times.” So again, **human error.**

VASTAAMO

PSYKOTERAPIAKESKUS Vastaamo.fi
PSYKOTERAPEUTIT - PSYKOLOGIT - PSYKIATRIT

- In October 2020, Finland saw a rather exceptional combination of hacking and extortion. The private company *Vastaamo*, which provides psychotherapy services in 23 communities, reported that it had become the target of a hacking attack or attacks. The hackers demanded a sizeable payment; otherwise the data on private clients would be published. When the company did not pay immediately, the clients received similar demands. Some paid and some saw their data made public.
- At this editing, some 25,000 clients have filed a criminal complaint. The number of clients whose data have been backed may be as high as 40,000. According to the company's managing director – now former - the breach was caused by *a string of human errors*, not only one human error.
- Those errors led to bankruptcy

FOLKSAM

Folksam
För allt du bryr dig om

Another, essentially similar case is the data leak reported by the Swedish insurance company Folksam in the beginning of November 2020. The data on about one million clients – including confidential data – had been distributed to a number of major network players. The problem was discovered as part of an internal audit. In reporting the incident, the company expressed its regret *that the processing of data had not been carried out entirely as it should have.*

Yet the serious question:

How is it possible that the cases I have just discussed are quite recent and international news magazines in the field feature plenty just like them?

Knowledge Management

First, “knowledge management”, a term bandied about since the millennium began, has been slow to take root as a true mindset in organizations. Where information systems are concerned, we can still pretty much speak of “ignorance management”. The way from “silent knowledge” to “knowledge management” and lastly” ignorance management” is full of gaps. And here, it is unfortunate that no general, all covering obligation to appoint **data protection officers** was imposed when the GDPR was adopted. Now the rather haphazard nature of the system is a considerable problem.

Time-consuming and expensive processes

- The second reason I would cite is that changing a particular information system is often a time-consuming and expensive process. The threshold for incorporating changes that improve data security is rather high. This consideration, coupled with traditional attitudes, can amount to a formidable obstacle. People are only processing data. Changes tend to be introduced only after something has happened.

Lacking Design Thinking

- The third reason, also a weighty one, would seem to be a lack of familiarity with design thinking. There is little or no planning of the often long road information will travel. **Pseudonymization** alone would be a big step forward in improving data security for personal data generally and for confidential data in particular.   And there should be clear **alarm signals** telling when the borders of acceptable are visible.

Auditing Gaps

Auditing is something which is not – not yet - so well known as one important part of information management from the legal point of view. We do need also **legal forensic methods** and experts like Cesare Maioli

BRUCE SCHNEIER
Data Security Theatre

Last comments

In concluding, I would venture to speculate that people who invoke human error in explaining failures to process personal data properly or who claim that processing was not done “quite right” are incompetent; they are in the wrong business. Sad to say but this is how things stand in the constitutional state, one which is supposed to respect human rights. The ethical foundation on which data protection legislation is built is lacking the ethical framework needed to protect it. As *Bruce Schneier* has described it, data security is a reality in print but often largely *theatre* elsewhere. We should take data security seriously as a **critical digital right**. And we should have a new **sophisticated security culture**.

The end