HUMAN ERROR AND DATA SECURITY

Ahti Saarenpää

Professor emeritus, University of Lapland, Faculty of Law, Institute for Law and Informatics, Yliopistonkatu 8, 96300 Rovaniemi ahti.saarenpaa@ulapland.fi

Keywords: ***Digital Rights, Data security, System errors, Path of Information, Security theatre***

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.*

1. Lots of errors

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.[1] 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. Forgiveness has a place in the area of law as well, but it finds more limited application. It is not a general term or condition attached to what we do. An illustrative example is a 2016 ruling of the European Court of Justice in a case where a party failed to meet a time limit for instituting proceedings. The Court stated that, according to established case-law, being excused for failing to meet a deadline requires shortcomings on the part of the institution setting the deadline as well.[2] An error resulting solely from the incompetence of one party cannot be excusable in a matter of such importance. [3]

---

1 The Finnish language uses a word more along the lines of "humane" for "human" in "human error". This linguistic misconception carries a strong assumption that the error may be excusable. See for example Nortamo, Inhimillinen erehdys, Helsingin Sanomat (HS) 30.03.1994 (in Finnish).

2 It is interesting in terms of *legal culture* to look at the attitudes toward deadlines in different countries and at different time. If you will permit me one example in lieu of detail: A few years ago, we had a case before the Disciplinary Board of the Finnish Bar Association where a young lawyer was taken aback that he had been reproached although he had filed an appeal "only 43 minutes" late. Our reproach stood, however.

3 SV Capital OÜ v European Banking Authority (EBA), C-577/15 P, point 59 : With regard to the fifth ground of appeal, alleging that SV Capital made an excusable error, it is apparent from the Court's case-law that, in the context of the European Union's rules on time limits for instituting proceedings, the concept of excusable error justifying a derogation from those rules can concern only exceptional circumstances in which, in particular, the conduct of the institution concerned has been, either alone or to a decisive extent, such as to give rise to a pardonable confusion in the mind of a party acting in good faith and displaying all the diligence required of a normally well-informed person.
In criminal law, there is a long history of legislation on mistake as to the unlawfulness of the act. I will not go into this here.

2. Information systems in the digital network society

In recent years in various contexts, I have emphasized that we have advanced from the Information Society to the *Network Society* or *Digital Network 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.[4] This transformation has also been observed to some extent at least in the digital strategy of the EU. [5]

Digitalization is a trend that is given a positive spin in official political parlance. Accordingly, descriptions of the strategy talk about Europe's digital future. It is something that one should have no reason to avoid.[6] In broad perspective this is undoubtedly the case. The days when people looked upon technology with hesitation are by and large behind us. Even the most conservative lawyers have given in and started making use of the digital environment. We have reached a stage of development where, given the environment we work in, most lawyers and administrative experts are – or should be – *digital lawyers*.[7]

At the same time, however, we have to remember that what we see is not a neutral development of tools and our working environment only. We must address questions of the kind of information, skills and attitudes the change requires.[8] On the level of the individual, resistance to changes and the related *information avoidance*[9] account for many of the problems the change seems to occasion. I will not go deeper into these here; this would go well beyond the scope of the article. What I will focus on is the reliability of *information systems*.

3. Trust and trustworthiness

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.[10]

Trustworthiness or, from the individual's point of view, confidence, is built from a number of different elements in order to achieve trust. This requirement, a time-honoured one, serves to guarantee the regular operation of different organizations and social systems and, more broadly, society itself. We expect and require credibility of the things being done and the people doing them, and of the information involved as well.

This basic – and in fact rather simple – principle of life in our society has run up against new challenges in the Digital Network Society with the era of data stores and digital information systems it has ushered in.

---

4 See for example Saarenpää, Legal welfare and legal planning in the network society, in Barzallo et al. (eds.), XVI Congreso Iberoamericano de Derecho e Informatica, (2012) tomo I pp. 47–69, (FIADI) and Saarenpää, Does Legal Informatics have a Method in the new Network Society? pp. 51–73 in Saarenpää, Wiatrowski (eds.), Society trapped in the Network. Does it have a Future? (2016).

5 See more on the EU Commission at ec.europa.eu/info/strategy_en.

6 See Shaping Europe's Digital Future, EU Commission February 2020.

7 As recently as 2017, in the Disciplinary Board of the Finnish Bar Association, we had to examine a complaint in which the attorney denied having made a mistake and claimed that the incorrect VAT rate "came from the computer".

8 See more Saarenpää, The Digital Lawyer. What skills are required of the lawyer in the Network Society? pp. 73–85 in Schweighofer, Kummer, Hötzendorfer (eds.), Kooperation – Co-operation, IRIS 2015.

9 About Information avoidance as shaping our own informational environment, see Golman, Hagmann, Loewenstein, Information Avoidance, Journal of Economic Literature, 55(1) 2017, 96–135.

10 See for example Luhmann, Familiarity, confidence, trust: problems and alternatives. in Gambetta (ed.) Trust: Making and breaking cooperative relations. Oxford: Basil Blackwell, 94–105. Cfr. on the conceptual level Pöysti, Luottamuksesta hallinnon automaattiseen päätöksentekoon, Festschrift Pekka Vihervuori 1950, 25/8, 2020, pp. 345–360.

In the new digital constitutional state, *the path information takes* involves far more than producing and storing traditional static documents. Digital Information systems are significantly more than technical tools and document storage facilities. The age of document-based data processing should be over. However, we still see damage being done due to outdated views.

When we think of information systems in terms of the path information takes, we see the absolute necessity of analysing the multidimensional complexity of those systems in the *design phase*. I will take the example of the design of a system for the electronic administration of justice. When we set out to build an electronic court system in the constitutional state, we have to give due consideration to the perspectives of at least the following actors: (1) the citizen, (2) legal services, (3) the courts, (4) enforcement, (5) the media and (6) IT.[11]

Even this brief list shows the long road those planning the system have ahead of them if they are to achieve a *design* that – if you pardon the expression – does justice to the path information will have to take in the digital environment. As much as we speak about new *digital rights*, we can and should speak about digital trust and digital trustworthiness.[12] The above list also gives an indication of the types of data security problems one might run into if data security is not implemented properly in the system. The adage, "Not too much, not too little" is clear enough but as an approach leaves far too much to chance. We have a lot of different access rights.[13] Playing a key role here of course, particularly in the Nordic countries, is the century-old principle of access to public documents. This is taking on new forms as government becomes digitized. Where desirable, access can be achieved using dynamic digital documents.[14]

Be things as they may, it still seems that in practice operating with the simplest – even rudimentary – data security tools is more the rule than the exception. As a case in point, at the beginning of 2020, the UK Information Commissioner´s Office estimated that a full 90% of the data security breaches reported were the result of *human error*.[15] However, there is good reason to ask whether the perspective in that assessment might be somewhat flawed. Is the human error really the acceptable reason in all those cases?

I will now go on to present four European cases which should never have happened – particularly given the confidential nature of the information involved. One of the cases is from Wales, the others from Finland and Sweden.

The Finnish Institute for Health and Welfare (THL), as a government institution, maintains a significant 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.[16] The Institute then stated that the lapse was a case of *human error*.[17]

---

[11] See Saarenpää, E-Justice and Network Society Some comments from the Finnish point of view, pp. 211–234, in Cerbena (ed), Perspectivas Brasileiras e Européias Em E-Justiça. See also Reiling Information Technology in the courts in Europe, pp 601–616, and Reiling Technology for Justice, How Information Technology can support Judicial Reform, passim.

[12] About digital rights generally, see Saarenpää, Digital Rights, pp 17–22, in Verantwortungsbewusste Digitalisierung. Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020.

[13] Cfr. Willinsky, The Access Principle. The Case for Open access to Research and Scholarship, passim.

[14] See deeply Talus, From simply sharing the cage to living together. Reconciling the right of public access documents with the protection of personal data in the European legal framework, passim. This doctoral dissertation book is giving an overview about the Nordic Access principle in relation to data protection.

[15] See. https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/.

[16] This case information comes from the prosecutor's decision to not bring charges. The decision resulted in the incident falling under the statute of limitations and thus no longer being actionable.

[17] https://thl.fi/en/web/thlfi-en/search-results?q=error.

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 afternoon 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."[18] So again *human error*.

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 writing, 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. [19] According to the company's managing director – now former – the breach was caused by a *string of human errors*, not only one human error.[20]

Another, essentially similar case is the data leak reported by the Swedish insurance company Folksam in the beginning of November 2020. The data on some 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*.[21]

These unfortunate cases indicate that the reliability of even large organizations where data security is concerned may still be limited. In such instances, it is difficult to build and maintain confidence. The basic principle that data protection and data security should serve people seems to be rather remote from the values guiding the work of the organizations involved.[22] And these are – a point worth emphasizing here – just a few examples of what is a broader spectrum of errors, even huge errors.

4. Let's take data security seriously – at long last

Data security is of course not a novel concern – not in the least. Information, in particular important information, has been protected in many ways. We only need to look at the time it has taken to go from requirements regarding the written form of various legal acts to the more general information security on computers and data systems we see today.

On that journey we have witnessed many baffling situations. For example, the OECD, which published Data Protection Guidelines in 1980 that guided much subsequent legislation, did not come out with guidelines on data security until 1992. Data security did not become established as a dimension of security in its own right.[23] And even as a facet of data protection it had a secondary role. For example, the first Finnish Personal Data file Act (1987) mentioned only the *appropriate protection* of data. At that time there was no express definition of data security in the law.[24] And the later Data Protection Act, enacted in response to the EU Personal Data

[18] https://phw.nhs.wales/news/public-health-wales-statement-on-data-breach.

[19] The number of clients affected can largely be explained by the fact that Kela – the Social Insurance Institution of Finland – paid compensation for patient visits to Vastaamo. In other words, Vastaamo had acquired a sort of semi-public status.

[20] At this writing it is plain that data security at the company was woefully poor but there is no detailed information available on it.

[21] https://nyhetsrum.folksam.se/sv/2020/11/03/folksam-anmaler-delning-av-personuppgifter-till-datainspektionen/.

[22] See GDPR recital 4: The processing of personal data should be designed to serve mankind…

[23] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) and Guidelines for the Security of Information Systems and Networks, Towards a Culture of Security (1992).

[24] One of the things we at the University of Lapland in the Institute for Legal Informatics referred to in a 1997 analysis of the need for data security legislation was "legislator risk". This was borne out: Our proposal was not approved by the Government. Saarenpää et al.,Tietoturvallisuus ja laki: näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä tutkimusraportti (1997) (in Finnish only).

Directive, still largely proceeded from the controller's determination of the relevance of processing. When reading it *without general principles tools* it was often understood a lot like soft law.

Given the state of legislation at that time and how slow we have been to realize the increased importance of information networks, it is no wonder that data security has been slighted and changes for the better have even met with resistance[25]. Today, things are quite different across the board. The increased importance of *human* and *fundamental rights*, as well as the new *digital information infrastructure* we rely on, force us now outright to take data security more seriously.[26] Along with information and data security, we talk about digital security and especially cybersecurity. The 2010s have seen efforts to promote it through discussion, regulation and supervision nationally as well as internationally. For example, the European Network and Information Security Agency *Enisa* started out as a temporary organization but has since been made permanent. And its official name reflects the development in regulation: *the European Union Agency for Cybersecurity*.

Yet the serious question: how is it possible that the cases discussed above are quite recent and international news magazines in the field feature plenty just like them?[27] I can see at least three basic explanations.

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.[28] And here, it is unfortunate that no general, all covering obligation to appoint d*ata protection officers* was imposed when the GDPR was adopted. Now the rather haphazard nature of the system is a considerable problem.

The second reason I would cite is that changing a particular information system is 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.

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 road information will travel. *Pseudonymizatio*n alone would be a big step forward in improving data security for personal data generally and for confidential data in particular.[29] And there should be clear alarm signals telling when the borders of acceptable are visible.

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.[30] *We should take data security seriously as a critical digital right*.

---

25 In 1991 the Finnish newspaper *Helsingin Sanomat* ran a news item that the Population Register Centre, which maintains central records on all Finns, had neglected to draw up a data security plan. The director of the Centre – a lawyer by the way – responded in a subsequent interview that data protection plans were nothing *but unnecessary bureaucracy.*

26 See Saarenpää, The Importance of Information Security in Safeguarding Human and Fundamental Rights (2008). For example, the first Finnish Data Protection Act spoke only of appropriate protection of data. Looked at today, this is a hollow expression. What is more, at the time the law had no express definition of data security.
About the steps toward data protection as a fundamental right see more Gonzales Fuster, Gloria Emergence of Personal Data Protection as a Fundamental right of the EU, passim 2014.

27 See for example https://cyware.com/cyber-security-news-articles.

28 See for example theoretically already Jäger – Weinzierl, Anthony Giddens in Anwendung: Theorie der Strukturierung als Theorie organisationalen Wandels – das Beispiel Wissensmanagement. In: Moderne soziologische Theorien und sozialer Wandel (2011).

29 See more Saarenpää Pseudonymous identifiability as a societal problem, passim in Schweighofer – Kummer – Saarenpää (eds.) Internet of things (2019).

30 Schneier Beyond Fear: Thinking Sensibly About Security in an Uncertain World (2006), passim. The expression "*security theatre*" is nowadays quite often used in international discussions of security.

Literature

Golman, Russell; Hagmann, David; Loewenstein, George F., Information Avoidance. Journal of Economic Literature, 55(1) 2017, pp. 96–135.

Gonzales Fuster, Gloria Emergence of Personal Data Protection as a Fundamental right of the EU, Springer Science & Business Media. 2014.

Jäger, Wieland; Weinzierl, Ulrike, Anthony Giddens in Anwendung: Theorie der Strukturierung als Theorie organisationalen Wandels – das Beispiel ‚Wissensmanagement'. In: Moderne soziologische Theorien und sozialer Wandel. VS Verlag für Sozialwissenschaften, Wiesbaden 2011.

Luhmann, Niklas, Familiarity, confidence, trust: problems and alternatives. pp 94–110 in Gambetta (ed) Trust: Making and breaking cooperative relations. Oxford: Basil Blackwell, 2000.

Pöysti, Tuomas, Luottamuksesta hallinnon automaattiseen päätöksentekoon, pp. 345–360 in festschrift Pekka Vihervuori 1950 – 25/8 – 2020, Suomalainen Lakimiesyhdistys 2020 (in Finnish).

Pöysti, Tuomas, Trust on Digital Administration and Platforms, in 50 years of Law and IT, Scandinavian Studies in Law, Vol. 65, 2018.

Reiling, Dory Information Technology in the courts in Europe pp in: Gottwald (hrsg.), e-Justice in Österreich, Erfahrungsberichte und europäischer Kontext, Festschrift für Martin Schneider Weblaw 2014.

Reiling Dory, Technology for Justice How Information Technology Can Support Judicial Reform Leiden, Amsterdam University Press, Leiden, Amsterdam 2009.

Saarenpää, Ahti, The Importance of Information Security in Safeguarding Human and Fundamental Rights, http://www.juridicum.su.se/Iri/e08/documentation/ahti_saarenpaa-information_security_and_human_rights-paper.pdf 2008

Saarenpää, Ahti, The Digital Lawyer. What skills are required of the lawyer in the Network Society? pp 73–85 in Schweighofer – Kummer –Hötzendorfer (Eds) Kooperation – Co-operation, IRIS 2015 Österreichische Computer Gesellschaft – Austrian Computer Society (2015).

Saarenpää, Ahti, Pseudonymous identifiability as a societal problem, pp. in Schweighofer – Kummer – Saarenpää (eds.) Internet of things, Tagungsband des 22. Internationalen Rechtsinformatik Symposions: IRIS 2019, Weblaw 2019.

Saarenpää, Ahti, Does Legal Informatics have a Method in the new Network Society?, pp 51–69, in Saarenpää, Wiatrowski (eds) Society Trapped in the Network Society. Does it have a future?, University of Lapland 2016.

Saarenpää, Ahti, Digital Rights pp 17–22 in Verantwortungsbewusste Digitalisierung. Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020. Weblaw 2020.

Saarenpää, Ahti, E-Justice and Network Society Some comments from the Finnish point of view pp. 211–234 in Cerbena (ed) Perspectivas Brasileiras e Européias Em. E-Justiça. Federal University of Paraná – Brazil 2016.

Schneier, Bruce, Beyond Fear: Thinking Sensibly About Security in an Uncertain World Springer Science & Business Media 2006.

Talus, Anu, From simply sharing the cage to living together. Reconciling the right of public access to documents with the protection of personal data in the European legal framework. University of Helsinki 2019.

Willinsky, John, The Access Principle. The Case for Open Access to Research and Scholarship, MIT Press Massachusetts 2006.