People analytics in private-law employment relationships

Proposals for a more effective enforcement of data protection law

1) What is people analytics and who is affected?

In the digital era, companies use people analytics as a means to systematically evaluate their human capital in order to increase corporate value. A vast number of employees are affected by people analytics in their daily working lives: in Switzerland, 65% of companies analyse their workforces using people analytics. We know this from an empirical quantitative online survey conducted among 158 companies by the author in interdisciplinary collaboration with social scientists. The numbers are similar in other central European countries and even higher in the UK and the USA. And the trend is growing. More recently, the Covid-19 pandemic has promoted remote working and, perhaps not surprisingly, a desire on the part of the employer to monitor employees in their home offices.

While companies praise the benefits of people analytics, such as more transparency and fairness in personnel decisions, improved performance, cost reduction or a boost of innovation, the risks often remain unaddressed. Such risks may entail violations of employee data privacy, stress related to micromanagement, and algorithm-based discrimination. With people analytics, employers accumulate data and knowledge, thereby gaining power over their employees to an unprecedented extent. This dynamic accentuates the power imbalance at work, which has always been typical for employment relationships. Not only individual employees face disadvantages; the collective right of employees to information and participation in matters of employee protection must be considered as well. Furthermore, society as a whole has a public interest in a fair and efficient regulation of data flows. If, for example, workers are systematically excluded from the labour market because of algorithmic discrimination, the social security systems and thus the general public bear the costs.

In order to understand the new level of intrusion that people analytics makes possible, its distinguishing features must be emphasised: ubiquity, interoperability, and a growing use of artificial intelligence. With ever smaller sensors and devices, such as mobile phones or wearable computers that can accompany an employee around the clock, data may be collected everywhere (*ubiquitously*). The various data processing systems are *interoperable*, which allows one to combine data sets and gain new insights about the employee that were previously not visible when data sets were held separately. Lastly, ever more powerful computational infrastructure is able to process data in real time, anticipate the future with predictive analytics, and fulfil non-repetitive tasks thanks to *growing artificial intelligence*.

2) Current data protection law does not sufficiently address the risks of people analytics

Since data are at stake, data protection law is indispensable for an adequate handling of the risks incurred through the use of people analytics. Other fields of law, such as employment and labour law, anti-discrimination norms, criminal provisions, and fundamental rights may help answer certain questions raised by people analytics. The study examines the Swiss legal framework, but draws numerous comparisons with the applicable law in the EU and the USA, resulting in findings that have general significance beyond national borders. The analysis of

data protection law with respect to people analytics shows that the law does not always sufficiently address the risks described. The author formulates three theses:

First, data protection law must be interpreted in a risk-oriented manner. Data protection law concretises the protection of privacy in relation to data processing. The majority of provisions deal with the processing of data. In other words, such provisions are process-oriented. This does not necessarily align with the purpose of data protection law, which is to protect individuals from infringements of or risks to their right to privacy (see e.g. article 1 Convention 108). Therefore, the *ratio legis* demands risk-orientation. The many process-oriented rules must be understood in a risk-oriented manner. The author, with the above-mentioned interdisciplinary research team, conducted five qualitative case studies in the field, comprising over 100 interviews with employers and employees. One observation was that practitioners lack confidence and expertise to assess the risks of their data processing activities. In response to this finding, the author developed risk assessment parameters to give practitioners a tool for guidance. Key indicators of elevated risk are: data processing in the phase of knowledge application (as opposed to knowledge acquisition); growth of power imbalance between data controller and data subject; use of interoperable systems which infer insights of which data subjects cannot be aware; targeted reference to persons (as opposed to processing for the performance of a purely technical function); and extended dimensions of processing activities.

Second, employee consent should not be used as the default legal basis or justification for data processing in the employment context. While the concept of consent is widely considered to be a cornerstone of data protection regimes worldwide, some reservations should be made for employment relationships. The voluntary nature of consent must be viewed critically, as the employee is likely to be dependent on the job and may feel under pressure because of the structural power discrepancy between employee and employer. In addition, individuals tend to be asked for consent too often, which leads to consent desensitisation, i.e. individuals consenting indifferently without pausing and reflecting or reading the privacy policies. Swiss jurisdiction further restricts the validity of consent of employees in that consenting to a processing of employee data that has no factual link to the employment is only possible if the processing is to the employee's benefit. In sum, valid employee consent can only be obtained in very rare cases. The concept of consent hardly contributes to employee autonomy or to the diminution of risks.

Third, private-law data protection is poorly enforced. In a world of ubiquitous data collection, interoperable systems and increasing artificial intelligence, individual employees do not have the resources to actively contribute to data protection enforcement by seeking remedies against their employers in the courts. Data protection authorities have become more powerful with the modernised Convention 108, the entry into force of GDPR, and the revision of Swiss data protection law, but in many cases, authorities can only intervene in retrospect when the violation of the law has already occurred. The collective rights of employee information and participation could contribute to preventative enforcement, but employee representatives are often insufficiently involved in the development of people analytics and such an omission of employee engagement is not sanctioned by the law.

3) Towards stronger data protection more firmly rooted in real citizens' lives

The lack of checks and balances, together with the improvable level of reflection of practitioners in risk assessment, destabilise the entire data protection legal system. What is required is a systematic policy approach to ensure that data protection provisions are actively lived in real-life people analytics projects. The author thus calls for a two-pillar concept, namely professionalisation and democratisation of data protection law. Professionalisation encompasses any measure that causes the employer to comply with data protection law from the start of data processing. Democratisation refers to any measure that grants control rights to the parties opposed to the employer in order to work towards compliance with data protection law. Professionalisation will lead to more trust, democratisation will push institutional controls in data protection law. Both pillars together will ensure that all data controllers, data subjects, affected groups and authorities will be actively involved in the processing activities. This will lead to stronger data protection more firmly rooted in real citizens' lives, and thus to a more effective enforcement of data protection law. This concept could be expanded beyond the realm of employment contexts to data protection law in general.

The author places the two pillars outlined in the context of the recent adaptions under modernised Convention 108, GDPR and the revised Swiss data protection act. For instance, the duty to carry out data protection impact assessments will cause the employer to reflect continuously about the risks of its processing activities so that, eventually, the employer will act more professionally. On the other hand, increased sanctioning powers bestowed on authorities lead to a democratic counterweight so that data controllers cannot act as independently as they did before.

The concept of a twinned professionalisation and democratisation goes further than what has already been suggested or implemented by policymakers. The author applies it to ideas explored in legal literature on this or the other side of the Atlantic and further develops such suggestions. Besides legal measures, his concept involves social aspects. For instance, professionalisation is improved by investments in training and education of data controllers. A technical side is also integral to the concept. For instance, democratisation can be promoted if individuals are equipped with technological tools to determine data processing, such as easy-to-handle internet browser settings. After all, professionalisation and democratisation involve a shift in mindset towards increased awareness of data protection. Reducing the countless policy efforts of recent years to one common denominator, the concept of professionalisation with democratisation, has the potential to simplify and streamline future policy debates.

* * * * *

The above is a summary of the applicant's doctoral thesis, accepted as a dissertation *summa cum laude* (with highest distinction) by the University of St Gallen in the autumn semester 2020. It is nominated for the prize of the Professor Walther Hug Foundation for the Promotion of Legal Research. The book will be available in early 2021 (ISBN 978-3-03891-273-6; open access-ISBN 978-3-03929-009-3; DOI https://doi.org/10.3256/978-3-03929-009-3, published by Dike Verlag AG).

The dissertation emerged from a research project funded by the Swiss National Science Foundation. Empirical data was collected in interdisciplinary collaboration with a team of legal scholars and social scientists from the fields of ethics and human resource management.