Trends I Strict enforcement: evidence obtained in breach of privacy law is inadmissible

The Dutch Supreme Court recently ruled that insurers have only a limited possibility to use evidence obtained in breach of privacy rules. This inadmissibility of evidence is in line with the recent trend of stricter civil law sanctioning for the violations of privacy law. In labour law cases, Dutch courts awarded immaterial damages to employees whose laptops and telephones have been searched by their employers in breach of privacy rules. The French Supreme Court invalidated a sales contract of a database not registered with the data protection authority. In Germany, various courts determined that competitors can directly invoke breach of privacy rules if a company's inadequate information to consumers leads to unfair competition. And as soon as the European General Data Protection Regulation is adopted, supervisory authorities will be able to impose higher fines – the current proposal is a maximum of EUR 100 million or 5% of annual worldwide turnover, whichever is higher.

Personal investigation criteria

In the dispute that led to the Supreme Court's decision, the insurer sued an insured party for the repayment of benefits under a disability insurance policy. The insurer also claimed compensation for costs incurred in carrying out an investigation involving observation of the insured. The insured argued that the results of this investigation should be disregarded as they had been obtained in breach of the 2004 Code of Conduct in Personal Investigations (2004 Code of Conduct) (*in Dutch only*) drawn up by the Dutch Association of Insurers.

The Supreme Court considered that personal investigation in principle violates the privacy of an insured and is unlawful, unless there are grounds for justifying it. In the case at hand, the insured's privacy had to be weighed against the insurer's interest in investigating and countering insurance fraud. As with any processing of personal data, the principles of proportionality and subsidiarity – as set out in the explanatory memorandum to the Dutch Data Protection Act (WBP) – must be applied in assessing these factors. As regards subsidiarity, the data controller must assess whether it can reasonably achieve the objectives of the processing in a manner that is less detrimental to the individual concerned. In the case at hand, however, both the court of appeal and the Supreme Court applied the principles of proportionality and subsidiarity as set out in the 2004 Code of Conduct rather than those in the WBP. The 2004 Code of Conduct required the data controller to verify whether a personal investigation was the only available method and thus imposed a stricter norm than the WBP. According to both courts, the subsidiarity principle in the 2004 Code of Conduct means that such a drastic measure as personal investigation should only be taken if there is no longer any point in seeking the insured's cooperation. But that point had not yet been reached and, consequently, the results of the investigation had been obtained unlawfully. It is not unlikely that the court would have reached the same outcome if it had applied a less strict test of the WBP. The 2004 Code of Conduct was amended in 2011 and now closely follows the WBP.

Inadmissibility of evidence

The next important issue in this case was whether unlawfully obtained evidence should be excluded. According to established case law, this is only possible if there are additional circumstances justifying exclusion. See, e.g., the recent decisions by the Supreme Court of 11 July 2014, and – in relation to the 2004 Code of Conduct – the decisions of the Leeuwarden- Arnhem Court of Appeal of 25 March 2014 and of the District Court of Rotterdam of 28 May 2014. The District Court of Amsterdam, however, ignored the requirement of additional circumstances in its decision of 2 January 2014.

In the case at hand, the court of appeal and the Supreme Court ruled that these additional circumstances were present: not only was the subsidiarity principle in general violated, but the objective of the insurer's self-regulation would also not be served by admitting evidence in breach of that self-regulation.

Notably, the court of appeal and the Supreme Court, in assessing the unlawfulness of the data processing and the exclusion of evidence, gave much weight to the wording of the 2004 Code of Conduct and to the fact that this was a form of self-regulation. It is unclear whether violating the organisation's 'own rules' was decisive and whether the violation of statutory norms alone would have been sufficient to rule evidence inadmissible. The court of appeal and the Supreme Court could have also directly referred to the WBP.

Stricter sanctions are the trend

Inadmissibility of evidence is in line with a current trend, seen both in the Netherlands and Europe, of having stricter civil law sanctions for privacy law violations. The Arnhem-Leeuwarden Court of Appeal ruled on 2 February 2014 that handing in a laptop by an employee for investigation does not imply the employee's consent to the accessing of all files on his laptop. The fact that the detective agency carrying out the investigation violated its own code of conduct was a major contributing factor in this case. In May 2014, the Amsterdam District Court awarded compensation for pain and suffering to an employee whose private Gmail accounts and WhatsApp messages had been accessed by the employer. According to the court, the employer's investigation was not based on a concrete suspicion that the employee was acting in breach of his employment. The investigation looked more like a fishing expedition that started after the employee informed his employer that he wanted to accept a position with a competitor.

It is notable that inadmissibility of evidence did not pay a role in the first case, whereas in the second case a request to exclude evidence was denied because there were no special circumstances to justify inadmissibility. In Dutch employment law, judges more frequently opt for awarding a (slightly) higher severance payment rather than excluding the evidence, partially

because continuing the employment is often no longer a realistic option.

In France, the highest court ruled in 2013 that a purchase agreement was invalid because the customer database that was part of the deal had not been registered with the privacy supervisory authority. In Germany, the higher regional court of Hamburg (*Oberlandesgericht Hamburg*) decided that a company should not gain a lead on its competitors by giving customers insufficient information about the use of their data. In this case, a producer of blood sugar tests had provided free tests without stating what it would do with the data collected. As in another similar German case, the court ruled that competitors may directly invoke the privacy rules and can accordingly block such promotional campaigns. And when the European General Data Protection Regulation is adopted, an additional sanction will be available: depending on the final text of the Regulation, fines of up to EUR 100 million or 5% of the company's annual worldwide turnover, whichever is higher, can be imposed.

Insurers should be careful in launching personal investigations when they suspect fraud. The Supreme Court leaves little scope to use evidence obtained in breach of privacy rules, whether the evidence is its own or not. The Supreme Court's ruling is in line with a clear European trend. Violation of privacy rules, irrespective of whether it is committed in an employment, insurance, commercial or competition context, could cause ever more serious problems for data controllers.