7. ECTA Articles

AUTHORS:

Tamara Moll

Attorney-at-Law

Cohausz&Florack

tmoll@cohausz-florack.de

Maria Boicova-Wynants

European Trade Mark Attorney,

IP strategy consultant, Partner

Wynants & Co

maria@wynants.eu

VERIFIER:

Nicole Ockl

Group Director IP Legal, Domains & Licences

Tui Group

nicole.ockl@tui.com

Guardians of Innovation: Navigating the Intersection of AI, Data Protection and Trade Secrets

In today's digital world, data management and trade secret (TS) protection are critical issues that may even converge (e.g. when personal data is part of a business secret, such as customer and supplier lists). AI and big data analytics tools can aggregate and process vast quantities of data, which may drive innovation, but could also put it at risk. A thoughtful and holistic approach to data management and TS protection is therefore becoming essential.

New Risks

AI and data mining tools excel at uncovering previously undetected or inadequately understood correlations within extensive and diverse datasets. These correlations can yield novel insights, unveiling patterns across various domains such as consumer behaviour, commodity pricing, labour markets, ongoing scientific endeavours, technological advancements, and regulatory landscapes. Predictive models further enable extrapolation of future scenarios, serving as invaluable planning aids for both enterprises and regulatory bodies.

Even when fully-compiled data is not publicly available, raw data points utilised for AI training or specific big data analyses may be accessible to individuals within similar industry circles, provided they possess the requisite licensing. Moreover, complex processes or products, regardless of intricacy, with the help of AI, become susceptible to rapid and cost-effective reverse engineering, rendering traditional TS protection more challenging and less reliable. The integration of independent discoveries facilitated by AI and big data analytics is considered lawful, unless access to the data itself is illicit. Furthermore, the practice of reverse engineering, when conducted within the confines of observing, studying, or testing a publicly available product, transforms into a legitimate form of acquisition. While conventional wisdom may suggest that few secrets can withstand such technological scrutiny in the future, the question remains: Can the existing legal framework for safeguarding TS provide adequate protection against these advancements?

In essence, the convergence of these legal and technological domains underscores the need for a nuanced understanding of how combining multiple lawfully acquired data sources through big data analytics can unravel TS in a lawful yet impactful manner. With that knowledge, it is possible to establish secrecy based on the undisclosed configuration or structure of the data set,

rather than the mere aggregation of its elements. This presents opportunities for trade secrecy by design.

The protections in place

The Trade Secrets Directive (Directive (EU) 2016/943, TS Directive) is the key piece of legislation protecting TS protection in Europe. The TS Directive safeguards against unlawful acquisition, use, and disclosure. As outlined in Recital 30 of the TS Directive, the scope of 'trade secret' encompasses both business and technological information, including know-how, provided that information has been kept appropriately confidential – while excluding trivial knowledge, employee-acquired expertise, and widely known information obtained in the ordinary course of business.

Data protection, with a primary emphasis on regulations such as the General Data Protection Regulation (GDPR), is fundamentally concerned with safeguarding personal data from any form of unauthorised processing. Conversely, the safeguarding of trade secrets revolves around shielding company information that holds substantial commercial value from illegitimate access, usage, or disclosure. Personal data, as defined by Art. 4 No. 1 of the GDPR, encompasses *'any information relating to an identified or identifiable natural person'.*

Although these two realms may seem distinct in their objectives, they intersect in significant ways. One notable point of convergence lies in the requisite technical and organisational measures mandated to ensure compliance and robust protection in both spheres. These measures play a dual role, serving not only to fortify the integrity of TS but also to bolster the framework of personal data protection.

Investigating the parallels

To protect a company's information as a TS, the legitimate owner must take appropriate confidentiality measures; in this respect, there is a parallel to the GDPR, which requires appropriate measures to protect personal data.[1] Whether the concept of appropriate measures to protect confidentiality, as used in the TS Directive, is the same as the concept of appropriate measures has not yet been fully clarified. However, both terms have one thing in common: the personal data or TS must first be identified and then categorised into risk classes. Classification is based on the following formula:

probability of occurrence × extent of damage = degree of risk

The reference point for measuring the extent of damage is linked to the economic significance of the loss of the TS for the company and the measures required to impose the legal consequences of the TS Directive on the infringer.

In the case of data protection, on the other hand, the relationship between the data controller (the company processing personal data) and the authorised party ('data subject') is the decisive point of reference regarding the extent of damage. While the protection of TS is based exclusively on the protection worthiness of the right holder and the potential infringer, the point of reference for data protection is the relationship between the data controller and the authorised party ('data subject'). The more important the information is for the authorised person, the more protective measures the controller must take to protect the information from access by third parties. The perspectives of data protection and the protection of TS therefore differ. However, both areas can benefit from each other, particularly concerning the necessary protection concepts and measures.

Added complexity for protecting real-time data

In line with other legal frameworks addressing data, the EU legislature adopts a static perspective regarding the concept of know-how and business information. While this approach aptly applies to static entities like chemical formulas or prototypes, it poses challenges when applied to dynamic real-time information associated with big data. In fact, within the specific context of AI and big data, the directive's static approach to information poses potential challenges in determining the adequacy of measures to meet the requisite due diligence threshold.

[1] Art. 22 (3) 1 GDPR ('suitable measures'), Art. 88 (2) GDPR ('suitable and specific measures'), Art. 9 (2) (g) GDPR ('suitable and specific measures') and Art. 32 (1) GDPR ('appropriate technical and organisational measures to ensure a level of security appropriate to the risk').

7. ECTA Articles

Real-time data holds significant commercial value, yet describing its precise configuration and composition, especially within the context of online data mining tools, may prove elusive. One interpretation could focus on categorising information under predefined criteria, regardless of its dynamic nature, thereby acknowledging the evolving informational content generated in real-time.

Protecting the trade secret information in AI applications

In view of the difficulties in protecting core components of AI applications (in particular algorithms, models, and raw and training data) under IP law, it is of central importance for companies to place AI solutions themselves under the protection of the TS Directive.

The first starting point for such TS protection for AI applications, in the narrower sense of the computer programme containing algorithms, is to share it with as few people as possible and, if necessary, to offer the programme as a software as a service (SaaS) solution and not as an installation at the customer's premises ('on site'). If, for example, cloud structures of a third-party provider are used to provide the SaaS solution, it must be ensured that the TS is also adequately protected by encryption and/or NDA.

Practical steps – assessing risk and devising strategy, technical and human solutions, integration with management systems

Existing systems and organisational structures for data protection can also help to meet the legal requirements for the protection of TS. Following the identification of both personal data and trade secrets, the next crucial step involves devising a tailored protection strategy for each. This strategy should be informed by the delineated protection categories and insights gleaned from the comprehensive risk assessment conducted. Firstly, the responsibilities within the company must be defined, for example by appointing a data protection officer or confidentiality officer. The next step is to determine the need for protection of the information and personal data and the corresponding risk classification. Protective measures must then be defined for the information or personal data that corresponds to the risk classification.

For information that is not personal but is considered a business secret, most of the technical and organisational protective measures that companies take for data protection under Art. 32 GDPR can also be applied. In particular, when determining suitable technical and organisational measures as required by Art. 32(1) GDPR, the company's experience and data protection documentation can be used to protect TS through technical and organisational measures.

Technical precautions are an essential element of protection. Ideally, business secrets are stored or filed in such a way that they cannot be accessed or searched without authorisation. The same applies to personal data. After all, what is not available cannot be processed or disclosed without authorisation. Typical technological measures that we are already familiar with from data protection include securing the IT infrastructure and data storage. Encryption, access and access controls, as well as regular security checks.

Nowadays, safeguarding TS increasingly relies on controlling even source information and seemingly trivial data. Compartmentalising key information among workers, collaborators, suppliers, clients, and the market is no longer sufficient in isolation. Technical measures must be supplemented by regular employee training and awareness programmes that instil a culture of confidentiality and enhance compliance with security protocols. In the area of organisational measures, we can fall back on measures that are also familiar from data protection, such as know-how protection guidelines, operating instructions, company agreements, IT security guidelines, and clean desk policies, to name but a few. In both areas, employee training is also necessary, ensuring that personnel are well-versed in the nuances of protecting sensitive information. Additionally, regular reviews and updates to existing measures, prompt interventions in case of breaches, and the implementation of a robust risk management plan are essential practices to uphold.

Finally, similar to data protection, TS protection may be integrated into existing management systems, such as ISO 9001 or ISO 27001. As AI evolves, businesses will encounter new opportunities and challenges, making it crucial to stay ahead of regulatory changes. Companies need to be vigilant, adapt strategies in line with legislative updates, and ensure their practices comply with data protection laws while harnessing AI's potential.

Key Take-Aways

In summary, the relationship between TS and data protection is more interconnected than initially perceived. Organisations can create a more secure and resilient environment by integrating TS protection strategies with other information security and data protection measures, adopting an overarching holistic approach to managing data. This can save time and effort by reducing duplication. Protecting both business information and personal data can strengthen an organisation's reputation and trustworthiness. As the digital era progresses, the convergence of TS protection and data protection is likely to become a cornerstone of corporate strategy.«