Source: *The Straits Times,* pA18
Date: 24 November 2020

'People analytics' – how to track workers from afar

The same technologies that make remote working possible also allow firms to legally monitor their employees. Singapore's recently introduced data literacy framework can help to raise awareness, but more needs to be done.

Andreas Deppeler
For The Straits Times

This year, the world of work changed beyond recognition. In Europe and the United States, more than 40 per cent of the labour force worked from home during the first wave of the Covid-19 pandemic.

In Singapore, droves of office workers deserted their high-rise towers in late March and early April and installed themselves at makeshift desks in their homes.

Many are still there. As the end of the year approaches, workplace closure measures remain in effect in most parts of the world.

Remote working has proven to be generally popular among employees. In a survey conducted in the European Union in July, almost 60 per cent of respondents said they were satisfied with their experience of working from home; 65 per cent said they would like to continue doing so at least several times a month, if given the choice.

In Singapore, eight out of 10 employees prefer to work from home or have flexible working arrangements, according to a recent survey commissioned by The Straits Times.

Among employers, reactions range from mildly sceptical to unabashedly supportive.

Mr Jamie Dimon, chief executive officer of investment bank JPMorgan Chase, noting that productivity has fallen, "especially on Mondays and Fridays", wants to slowly bring some staff back to the office.

At Microsoft, according to recently issued guidance, working from home part of the time is now viewed as "standard" for most roles. Mr Jack Dorsey, CEO of Twitter, told employees in May that they would be allowed to work from home "forever".

MONITORING THIS WORKFORCE

As workers divide their time between employer premises, client sites, coffee shops, subway trains and their homes, how are firms tracking their performance and productivity?

As it turns out, the same information and communication technologies – the Internet, computers, mobile phones, wearable devices – that make remote working possible also allow firms to monitor their staff.

In fact, "people analytics" (as it is called) has been a major trend in human resource (HR) management for several years.

The objective of people analytics is, to put it simply, to collect large amounts of digital data about the workforce and transform this data into statistics, patterns, predictions and insights with the help of computational tools that are often referred to as machine learning or artificial intelligence (AI).

Data is mined from collaboration and productivity applications used within the firm; aggregated with geolocation and metadata from mobile devices and sensors; and further enriched with public information harvested from external sources, in particular social media such as Facebook, Instagram, Twitter and LinkedIn.

To illustrate how people analytics can be applied, let us assume that a company wants to measure "employee engagement", a term that is beloved by HR professionals, consultants and managers although almost nobody knows what it means.

According to professor of organisational behaviour William Kahn, who introduced the concept, people who are engaged "employ and express themselves physically, cognitively and emotionally" while at work.

Conversely, when employees are disengaged, they withdraw and "uncouple" their selves from work roles. Clearly, companies want their workers to be engaged.

Traditionally, firms have conducted annual or biennial surveys in which they ask their employees to rank certain statements (such as "My job provides me with a sense of meaning and purpose") on a scale from one to five.

Their answers are then aggregated into a so-called "engagement score". Needless to say, the empirical validity of this approach is highly contested.

In contrast, in the brave new world of people analytics, algorithms continuously extract and analyse employee data to infer changes and trends in behaviour, attitude and sentiment.

For example, based on statistical analysis of e-mails exchanged, documents produced, Web searches, login times, LinkedIn posts and many other bits and bytes left behind in the digital data trail, an AI engine may conclude that an employee has "disengaged" or is "at risk" of doing so.

HR and management are promptly alerted and can take corrective or pre-emptive action.

Amid the pandemic, many Singaporeans no longer work in their physical offices but at home. The writer says the digital tools they use also produce data that can be tapped by others to make inferences about them. ST PHOTO: KELVIN CHNG

SURVEILLANCE CAPITALISM AT WORK

According to a recent report by consulting firm McKinsey, most large organisations use people analytics; 70 per cent of executives view it as a top priority.

As it happens, extracting large, unstructured, real-time data ("big data") from users and turning this into aggregated statistical predictions that can be sold to advertisers has been the core business model of digital platform companies such as Google, Facebook, Amazon and Tencent for more than 15 years.

Viewed in this way, people analytics is just another variation of what former Harvard professor Shoshana Zuboff calls "surveillance capitalism".

As she describes it in her book The Age Of Surveillance Capitalism, the ultimate objective of digital platforms (or corporate HR departments for that matter) is to shape user (or employee) behaviour towards maximum profitability and compliance.

Defenders point to the supposed "neutrality" and "rationality" of data-driven decision-making. Studies have demonstrated, however, that algorithms can inherit human biases. At its worst, the unquestioned, uncritical use of algorithms (for example, in recruiting, or performance management) can perpetuate and amplify the very biases that adopters of AI technology were hoping to eradicate.

LIMITS OF THE LAW

Can workers rely on the law to protect them against seemingly limitless surveillance?

Legal instruments, such as the European General Data Protection Regulation (GDPR) and Singapore's Personal Data Protection Act (PDPA), do give some control to individuals over how their data is used. Both require companies to seek consent from individuals to have their personal data processed for a specific purpose.

However, firms can easily obtain consent by having employees and applicants sign a "Data Protection Policy". Furthermore, neither GDPR nor PDPA imposes significant restrictions on the use of machine learning and AI to inform decisions about employees. As a result, people analytics and employee surveillance, while ethically questionable, are (for the most part) perfectly legal.

What if, instead of trying to curtail the data analytics practices of employers, we regulate those that operate the data and AI infrastructure through which surveillance is conducted – in other words, big technology firms? An example of such an attempt is a civil lawsuit filed by the US Department of Justice against Google last month.

Antitrust law in the United States, beginning with the 1890 Sherman Act, was crafted to deal with monopolies in clearly delineated industries such as rail transport, oil and steel production, and telecommunications – not with digital platforms whose virtual supply chains spread across the entire world.

Many, therefore, expect the Google lawsuit to reach a similar conclusion as the one brought against Microsoft in 1998: a slap on the wrist, minor changes to business practices and governance structure, and no further consequences.

NEED FOR DATA LITERACY

Privacy and antitrust legislation everywhere seem inadequate to rein in large-scale surveillance and algorithmic profiling by organisations.

As this year has made clear, most of us depend on digital tools to work and participate in society. Through these tools, we produce large amounts of data that can be garnered and used by others to make statistical inferences about us. But even as our everyday lives become increasingly visible to organisations, their surveillance operations remain largely invisible to us.

While people are generally aware that information is gathered about them, most are unaware of the inner workings and economic imperatives of continuous data extraction, aggregation, profiling and monitoring.

This makes them vulnerable to misinformation, manipulation and psychological harm. What is needed, therefore, are policy interventions to build what scholars call "critical data literacy": the ability to recognise and critically reflect on the benefits and risks of data collection and advanced analytics.

In Singapore, initial steps towards that goal have been taken with the launch last year of the Digital Media and Information Literacy Framework by the Ministry of Communications and Information.

The current version of the framework covers topics such as digital advertising, misinformation, data protection and cyber security. It also briefly explains how algorithms can exploit cognitive biases to influence thinking and online behaviour, but it stops short of addressing the wider ramifications of surveillance capitalism.

Endowing citizens with critical data literacy will, in itself, not do much to restore the balance of power between those that own the means of cognition and those whose behavioural surplus is extracted.

But, at the very least, it allows an informed debate about the kind of surveillance technology we want to admit into our workplaces and, by extension, into our lives.

stopinion@sph.com.sg

• Andreas Deppeler is adjunct associate professor and deputy director of the Centre on AI Technology for Humankind at the National University of Singapore's Business School. He teaches and writes about the economic and societal impact of technology.