AI will not replace engineers any time soon, says ING

Tech platforms must do more to stop scams, according to CTO. Aliya Shibli reports

ING's chief technology officer is a "mechanical engineer by mistake" who began coding at 11 years old before going on to study engineering. Daniele Tonella joined ING as the group's CTO in 2024 and oversees "everything that is technology" across the bank, which has around 19,000 tech-focused employees.

The Dutch lender operates large tech hubs in the Philippines, Romania and Poland. It opened a hub in Turkey last year and plans to open a new tech hub in Spain this year.

"Hiring in certain areas gives us access to pools of engineers which are simply bigger than in other places. That's the advantage we are looking into," he says.

As ING's tech hubs evolve into resource pools with specific skillsets, such as on-call engineers and security services, "they are becoming more mature, where some services are fully managed out of some locations", Tonella says.

The latest iteration comes around a decade after the bank started its digital-first journey, influenced by its heritage as a digital bank "before neobanks were a thing", he says.

A step ahead of AI-enabled fraud

Employee training, phishing simulations and filtering technology are among ING's tools to counter the growing threat of deepfakes.

"We see legislation starting to evolve, especially in the Nordics, where banks are being made more and more accountable in front of courts for these types of [phishing] situations that their clients incur," Tonella says.

Last year an ING employee received instructions in a voicemail impersonating the bank's chief executive, Steven van Rijswijk, which Tonella described as "a good learning moment".

But the intermediaries in these scenarios should take more action, he adds, referring to the tech firms, such as video call platforms, where scams can originate.

"I imagine that these providers have more information about who is trying to reach out to whom. But today, I don't have the impression that this is really very actively taken care of. All of these communication intermediaries probably need to evolve," Tonella says.

For other forms of impersonation fraud, ING has developed a security feature in its mobile banking app to help customers verify whether an incoming call is genuinely from the bank.

When customers receive a call claiming to be from ING, they can use an "is ING calling me?" button in their mobile banking app. After entering the caller's phone number, the app confirms whether the call is legitimate.

Career history

2024
Chief technology officer, ING

2021
Senior adviser, various organisations

2017
Chief executive, UniCredit Services

2013
Chief executive, Axa Tech

Since its implementation in the Netherlands in April last year — where it was developed — the tool has reduced fraud cases where scammers target customers by telephone impersonating ING by 50 per cent.

With the feature expanded to Poland and Italy last year, Belgium in May and Spain in June, ING plans to roll it out further.

"That feature can be adopted by other countries very, very quickly because of our single mobile app framework," Tonella says.

Elsewhere, the CTO is conscious that the reality of using AI must be separated from "bombastic" marketing claims. "That's not to say there is no value [and] impact. There is a huge one, but it's not as big as it seems when you hear the declarations. This is where we are navigating," he says.

Generative AI's pitfalls were clear during a recent incident whereby an AI co-pilot designed to intercept bugs in ING's code failed to notice the bug, likely because the deployment of the code was in multiple files that went into production at the same time, Tonella says. "At that moment, the co-pilot did not see it. So these types of experiences are where the marketing of AI hits reality," Tonella says. "We don't see yet a fleet of AI agents taking over end-to-end, unsupervised by humans. We just don't see it, at least not in engineering."

Cloud or fog?

Tonella expects more conversation around public cloud services, influenced by geopolitical dynamics.

There is growing concern about the geopolitical risks tied to digital service dependencies, such as public cloud platforms and satellite internet, he says.

"What is the regulator going to do in that space? Are we going to be forced to exit from non-European cloud providers?"

"It is a fog that at some point needs to be cleared out, because it's creating a lot of confusion inside the organisation, and makes long-term strategies a bit more difficult," Tonella says.

Events like satellite internet company Starlink's contested service availability in Ukraine highlight how critical tech services can be disrupted or "weaponised".

Generally, European banks' dependencies are highest in software-as-a-service platforms or cyber security tools — often from non-European providers — and less so in basic cloud infrastructure, he says.

The Trump administration has also created some "uncertainty" about the stability of the supply of cloud services.

"It's not that we can't have this product or the service provider, but it's more about how do we protect our data, and how do we protect our agility and ability to move around," Tonella says.

Some providers are responding with efforts like sovereign cloud offerings in Europe, but the underlying strategic vulnerability remains, he says.

While questions about existing dependencies have always been relevant, Tonella says the "perception of the risk of continuity of supply" has changed.

"Can that be weaponised? That's the question that is in the air."