记者|张晓云

近日，《反电信网络诈骗法》获得全国人大常委会审议通过，并将于2022年12月1日起正式实施。法案明确规定了公安机关、监管机构、金融机构、运营商、互联网服务商等各方的相关主体责任，强调全链条防范治理电信网络，为反电信网络诈骗工作提供有力法律支撑。

进入数字经济时代，电信诈骗的手段也日渐数字化，它们借助区块链、虚拟货币、人工智能、GOIP、远程操控、共享屏幕等新技术，不断进化，对金融安全生态发展带来全新的挑战。

坏人“数字化”了，我们的账户安全怎么办？来自电信、互联网、银行等机构单位的“反诈看门人”如何看待新型数字化诈骗？

魔高一尺、道高一丈，在日前举办的2022世界人工智能大会“数字灯塔 安全护航”数字账户安全特色论坛上，多位业内专家就当前的业务实践、行业痛点及前沿技术展开分享与交流，探讨以协同方式促进行业智联，共建安心、稳定、可靠的数字治理体系。

“从诈骗的角度来看，更精准化、更数字化的诈骗手段越来越多。”中国电信上海公司网信安部总经理傅伊浩表示，从通讯运营商的角度来看，目前的诈骗主要有两个特点：

一是新通讯工具的使用越来越广泛，传统靠电话来诈骗的比例逐年下降，通过一些互联网APP、网站来诈骗的形式不断增多，例如微信、QQ、钉钉，均有可能被诈骗分子利用，他们可以通过屏幕共享实现信息的获取，进而达到诈骗的目的。

二是诈骗手段越来越隐蔽，诈骗分子同时引入了新设备，像拨号设备从现场变成远程进行操作。

据介绍，新型数字化网络电信诈骗风险涉及面极广，涵盖公安、监管机构、金融机构、电信运营商、互联网平台服务商等各个环节，而出于信息安全的考虑，多方数据融合在金融账户风险识别上面临挑战。

“所有的犯罪都有犯罪三角形，即犯罪的动机、能力、机会，只要破坏了其中的一个角其实就不会有犯罪了。”基于这个理念，万事网联风险管理条线负责人Kevin Lau提出了一个策略，即预防、识别、政策与协作。

傅伊浩也认为，建立这样一个联防联控的机制非常重要。“怎么把整个链条串起来

？怎么进行端到端的考虑？面临一些用户个人信息保护的问题，怎么去做数据拦截的一些工作，这里也有一些矛盾。”

傅伊浩指出，其中涉及到一些新手段，目前保护个人信息方面有很多联邦算法、联邦计算来规避泄露用户风险，又能够通过数据分析把结果分析出来，这一块后续可能是重点。对于一些新技术的应用，规避一些政策上的风险，但又要更精准地识别，都是整个跨行业生态圈里面要着重研究的问题。

“当我们在研究诈骗分子，诈骗分子也在用先进的技术和专门的算法团队在研究我们的反诈模型。”中银金科助理总经理陈志表示，面对迭代迅速的新型数字化诈骗团队，传统风控策略已无法完全满足，银行必须采用新的数字化、智能化防控手段。

“人工智能本质上是机器学习算法，AI会学习，人可以通过制定规则的办法把人的经验教给它，AI还会根据不断产生的数据学习迭代。”氪信科技创始人兼首席执行官朱明杰表示，“始于人工，归于智能。应对新型数字化风险挑战，AI是最佳解决方案。通过将风控专家经验教给AI系统，金融机构能极大程度节约审核人力，同时AI的自迭代性完美适配与人脑及动态环境博弈对抗的新型金融场景。”

据介绍，氪信科技依托前期经验推出领航-TAI反电信网络诈骗风险管理产品，借助于金融机构内覆盖客户全生命周期的数据，动态灵活地将开户、使用、交易、风险等信息进行整合使用，对涉案账户进行有效事前预警和精准识别，助力金融机构对各类数字化诈骗的全面防控，保障金融数字账户安全。

除了技术层次的保障，金融数字领域生态圈也亟需协同合作，搭建安全的金融数字治理体系。“让数据可用不可见、使用可控可计量，多方数据协同必须借助SPU（Secure Processing Unit）机密计算。”粤港澳大湾区数字经济研究院AI安全普惠系统研究中心讲席科学家王嘉平称，希望机密计算能帮助打破目前数据孤岛的局势，让信息数据能安全地运用于多方。

借助于机密计算等底层技术，粤港澳大湾区数字经济研究院与氪信科技共同提出“数字灯塔”生态构想，旨在联通公安、电信和金融机构等多部门的信息数据，编织出一张反电信网络诈骗的数字化智能网络，用AI算法辅助专业决策，推动城市数字化治理的安全与发展。