两会 | 聚焦

□法治报记者 陈颖婷 胡蝶飞

随着大数据、人工智能、互联网新技术的广泛使用，隐私保护和数据安全问题日益突出，出现了一些个人信息被非法获取、泄露、滥用、甚至倒卖的现象。在大力推进数字化经济发展的同时，如何用好数据，管好数据，如何保护好公民个人信息等数据安全问题，成为今年全国“两会”代表委员们关注的焦点。部分在沪全国人大代表和全国政协委员就多个应用场景内的数据安全保障，提供了自己的真知灼见。

数据安全如何筑起“防火墙”

【商业】

移动支付应当再加“码”

移动支付已经成为许多国人的支付习惯。但支付便捷的同时，安全性也应引起思考。全国人大代表、致公党中央委员、上海市委专职副主委邵志清针对增强移动支付安全性提出一些建议。他认为移动支付为群众带来便利性的同时，也带来一定的风险性，对“短信验证码”的过分信任就是一个值得注意的隐患。为此，他建议适当限制短信验证码的功能并叠加更多身份核验手段，才能有效提高移动支付的安全性。

邵志清介绍，如今许多机构和平台在手机上凭短信验证码就能完成服务。但短信验证码的安全性级别相对较低，不法分子通过盗窃手机卡、拦截短信、武力胁迫等手段，获取并凭借短信验证码登录社保账户、公积金账户、银行卡账户和各类第三方支付平台账号，然后查询用户身份信息、银行卡信息等，修改账户密码和交易密码，盗刷银行卡并申请网络贷款。

针对这些问题，邵志清建议，首先要对短信验证码的部分功能进行适当限制。修改银行卡关联手机号、修改银行卡交易密码、银行卡解除挂失时，必须由持卡人持身份证至银行柜台办理；手机卡解除挂失时，必须由卡主持身份证至电信营业厅办理。“解除挂失是偶发事件，这样做既能更好保证卡主的安全利益，也没有造成太多不便利。”

其次，在短信验证码基础上叠加更多身份核验手段，如“人脸识别”或“私密问题验证”等技术，确保登录操作者是卡主本人；对于社保卡和公积金账户的登录，也应该设置同样的规则。

此外，为应对在绑架和抢劫等案件中，犯罪分子逼迫受害人交出密码、短信验证码和完成人脸识别的情况，邵志清建议利用“私密问题验证”技术对抗，建议允许卡主针对私密问题设置两个私密答案，一个是正常答案，一个为报警答案。用户输入两个答案都能完成移动支付交易，但如果是报警答案，银行和支付平台应该立即启动报警应对机制，拖延交易资金进入对方账户的时间，并立即通知警方跟踪资金流向等。

全国人大代表邵志清

【出行】

智能网联汽车更需关注信息安全

智能网联汽车因为其更为“聪明”，而备受期待。但由此可能产生的汽车信息安全事件同样不容忽视。

全国人大代表、上海汽车集团股份有限公司党委书记、董事长陈虹就数字生态环境下汽车数据安全和隐私保护提出了建议。

陈虹代表指出，目前智能网联汽车的数据采集和存储方面的责任和规范要求不明确，数据的商业用途约束要求不清晰。同时，对于数据泄漏的防范不足，需要针对数据泄漏风险建立法规制度和产业标准。与风险相比，现在对于数据违法的处罚力度不够。陈虹表示，国内目前对于个人隐私数据被侵犯的处罚力度相对温和，一般是处以警告和勒令整改，较为严重的也仅是处以几万元的罚款，没有惩罚性的处罚机制和被侵害对象的群体赔偿制度。

陈虹建议，规范和完善数字生态下的汽车数据保护体系。首先，建立准入制度：智能网联汽车数据（包括高精地图数据）的采集、存储和商业用途需经国家相关部门备案管理。数据安全和隐私保护对于智能网联汽车能否在国内销售应该起到决定性作用，只有符合要求的智能网联汽车产品才能进入汽车公告目录。

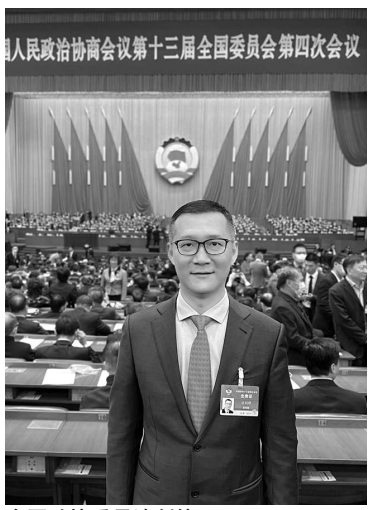
其次，加强对数据隐私保护。智能网联汽车企业对于可能存在的隐私风险具有告知义务，并且在收集、使用、转移、删除数据时给用户适当的自由选择权。同时，企业也需要提升软件的安全性，在分析处理数据时要进行数据和个人身份的分离，并将数据匿名化以确保数据的安全。用户对于他们的个人数据以何种目的被使用应该具有有效的知情权和选择权。

第三，建立过程审查制度。应当要求智能网联汽车的制造和销售企业建立完备的数据安全管理和软件升级流程。同时借鉴互联网信息管理制度，对智能网联汽车提供的数字服务内容也需要接受政府部门的监管和审查，并对所涉及的敏感数据及个人隐私数据出境问题作出明确的规定。

第四，严惩违法违规行为。相关部门应当严格执行数据保护相关的法律法规。对于危害或滥用涉及国家安全以及用户隐私数据的行为，应制定惩罚性措施和群体赔偿机制。

【立法】

规范数据采集应用 专设机构统一监管



全国政协委员谈剑锋

身为上海市信息安全行业协会会长，全国政协委员谈剑锋一直持续关注数据安全。“我可能是最早关注人脸识别数据安全的委员之一了。”谈剑锋告诉记者，今年全国两会上他一共有6个提案，其中5个与数据安全相关，这已经是他连续第四年递交相关提案。

“再这样下去，我们就快没‘脸’了。”谈剑锋说，“在海量的数据中，有些关键数据，如个人生物特征数据（人脸、指纹、DNA等），具有唯一性和不可再生性特征，一旦被窃取，无法追回并变更，对个人隐私保护将带来极大的、不可逆的风险。”而大量的国民个人医疗档案、健康档案汇聚后，可以用于分析该国的劳动力状况和经济、相关产业发展趋势，一旦被敌对势力获取，对国家安全和产业经济发展可能带来不可预估的危害。

谈剑锋表示，在大力推进数字化经济发展，鼓励大数据应用和创新的过程中，必须慎重考虑数据的分类分级和管控。

为此，谈剑锋提案建议，要加快相关法规制度建设，严格规范和落实关键数据的采集、存储和使用；要在法律框架下明确国家、集体、个人的数据权益，制定数据资源确权、开放、流通、交易相关制度，完善数据产权保护制度。同时建立数据分级分类管理的制度，对具有唯一特征的不可再生性数据的采集、传输、存储、使用必须加以严格控制；要制定负面清单，明确禁止一些生物、医疗等关键领域内的数据在互联网上的应用，切断风险源头。

谈剑锋还建议，相关部门须加强数据治理和数据监管，严控大数据的使用场景。要对互联网企业的信息采集进行严格的管理规定，只可针对企业产品的特性进行相关必要的数据采集，不得过度、无序、随意地采集；警惕互联网科技巨头的集中“巨头式”数据采集与应用。

“关键数据不可让企业自行采集收集，更不可由互联网龙头企业垄断。”谈剑锋表示，市场化公司具有天生的逐利本性，不可再生关键数据一旦被企业大量汇聚，很难保证其不被恶意窃取和所谓的创新利用。

此外，谈剑锋还建议设立国家“数据银行”，由国家成立专门机构，加强对不可再生的关键数据的统一管控，以最大程度地保障关键数据安全和国家安全。他认为，比如生物特征、人脸指纹、虹膜等数据，DNA数据、医疗和健康档案数据，必须由国家统一管理，市场不得自行采集、存储和使用。而国家应该统一管理的这些敏感数据，通过脱敏加密技术标识后再运用。

【管理】

“人脸识别”应持证上岗 实施许可证管理

无独有偶，全国政协委员、致公党上海市委专职副主委马进也十分关注“人脸识别”的采集与保存的安全。今年两会上，他递交提案建议，对人脸采集单位实施许可证管理。

具体而言，相关部门应出台人脸采集使用场景的限制性规定，并根据该规定就特定场所人脸采集的必要性、合理性以及场所所属企业的技术能力与管理能力进行评估，对符合条件的企业与场所颁发许可证。

“取得许可证后，企业才可在规定的场景下进行人脸采集。”马进说。在场景应用阶段，取得许可证的单位应尽到告知义务，赋予用户知情权和选择权。包括将许可证在指定场所显眼处公示，说明该场所采集人脸使用范围及必要性等。

此外，马进还建议，政府层面要做好监督与宣传两方面的工作，除了加强对于个人人脸信息隐私安全的宣传与教育，提高居民对于个人隐私权保护的意识外，可由用户协助共同监督，若发现有违规或强制采集个人人脸信息的行为，可通过有效渠道向有关部门反映。

全国政协委员马进