认，但并没有打消人们的疑虑。与此同时，许多民众对人工智能算法下的定向广告推送持负面看法。最经典的一个案例是，十年前一位网友因好奇心作祟在某购物软件上搜索“棺材”，没想到被“骨灰盒”的广告骚扰了一个月。现在的精准推送，比十年前有过之而无不及。

自 2016 年“剑桥分析公司”丑闻曝光以来，公众对社交媒体平台的质疑和担忧与日俱增。但是，在另一方面，绝大部分的人如今又都无法避免使用社交媒体，日常沟通联络、工作学习、购物娱乐和资讯传播等几乎都与这些平台相关。“既不相信，又无法摆脱”的困境正日益侵蚀着数字时代的广泛信任基础，进而衍生出更多社会问题。

数字时代，新兴技术的应用导致“个人数据”的边界日益模糊。大量涉及个人信息的数据正不断被抽取、拆分、汇合成支撑社会持续运转的庞大信息流，导致按照传统原则划分个人数据权利边界的难度明显增加。“一个最简单的例子，现在大家都觉得刷脸进小区非常方便，可是这些涉及你绝对隐私的信息就保存在小区物业的机器上，就是一般的人都可以轻易盗取，别说高级黑客了。这些信息到底该怎么保存怎么使用，大家还缺少共识。”崔久强说。

去年 11 月以来，以 ChatGPT 为代表的生成式人工智能等新技术、新业务的发布，引发行业变革，但也为数据安全保护和监管带来新挑战。崔久强指出，除了用 AIGC（生成式人工智能）伪造图像之外，大模型中隐含着许多敏感数据。不久前韩国三星一技术人员因写代码受困，求助于 ChatGPT，将企业生产的核心代码也上传了，使个人、企业及国家敏感数据不断处于风险之下。因此，如何做好数据的防泄密以及统一的数据管控，非常关键。

我们都知道区块链技术是一种分布式、去中心化的信任机制建立，借助于区块链技术可以实现数据和信息的不可篡改和可追溯性，从而确保数字信息的真实性和可靠性，为数字信任的技术实现提供了可行性的路径。这一特性使得区块链技术在数字信任领域具有广泛的应用前景，包括身份认证、数据管理、供应链管理和金融交易等领域。

“利用区块链的特性，有人做奢侈品、钻石珠宝的溯源。本来这是一个让买家觉得更加安全可信的交易方式，但是如果上链的数据就是假的，这不是更助长了奢侈品的造假吗？”崔久强指出，这就对监管提出了更高的要求。更别说如果是被假数据训练出来的大模型，那得出的结论得错得多离谱？

中国科学技术大学教授左晓栋分享了一个关于数据泄密的案例，更加凸显了数据问题的复杂性。在去年国家安全日之前，《焦点访谈》节目披露了一个案件，境外机构和境内机构相勾结，由境内机构在高铁沿线放置信号采集设备，窃取高铁运行数据，后来案子破获。此案被誉为《数据安全法》实施以来，首例涉案数据被鉴定为情报的事例，同时涉案人员被定罪为为境外提供非法情报罪。

当时有人疑问，高铁运行信号为什么要被称为情报，原因是什么？或者说背后的逻辑是什么？实际上这也是无奈之举。我们翻遍刑法，没有适用于这个案例的罪名。《刑法》有关窃取国家相关秘密的罪名，但是高铁数据不是国家秘密，《刑法》后来为了保护个人信息有侵害公民信息罪，但是高铁数据显然也不是个人信息，怎么办？但是它危害国家安全了，最近的罪名就是“情报”。“这说明在我们现有的制度设计，包括法律法规中我们对于数据安全保护的重点还不够。再确切一点说，我们以前认为这个数据影响了国家安全，毫无疑问那就是国家秘密。问题是，非国家秘密中是不是有影响国家安全的数据？是不是应当加以保护？这个问题自然就产生了。”

事实上，在当前千行百业的数字化转型中，无论是数据的复杂度，还是信任主体的类型与数量，抑或是各种新老场景对于数字信任的需求，均远胜过往。这意味着过去的数字信任建设模式、单独一个产品或者一个基础设施，很难匹配上数字化转型的长期需求。

> 在当前千行百业的数字化转型中，**无论是数据的复杂度，还是信任主体的类型与数量，抑或是各种新老场景对于数字信任的需求，均远胜过往。**

如何建立数字信任？

无论是政府企业，还是普通市