大数据下信息通信技术中的隐私保护研究

薛继军
国家乌海能源信息技术有限公司　内蒙古　乌海　016043

摘　要：随着我国大数据信息技术的不断完善，社会各界人士开始高度关注到信息通信方面的隐私安全保护工作。大数据时代的来临既是一个机遇，也是一个挑战，用户数据信息将会面临侵犯风险，导致在通信过程中发生数据信息被盗丢失的现象，严重侵犯到用户切身利益。因此，现代通信运营机构必须高度重视用户数据信息隐私保护工作，要及时采取有效措施，全面提高用户隐私保护能力。

关键词：大数据；信息通信技术；隐私保护

引言：近年来，大数据技术的不断发展为我们的生活、工作和学习提供了方便，对我们的思维方式也进行了重塑。在大数据背景下，数据信息的处理速度得到了提高，传统的信息处理技术得到了革新。企业可以通过大数据技术对企业的内部信息更加轻易的进行存储，个人在使用计算机时，对信息的搜索和获取也更加的方便。然而，大数据技术的发展也给信息通信的安全性带来了风险和挑战。

1 大数据与信息通信技术的关系

随着信息技术的快速进步，数据越来越多地影响着各个产业和社会的发展。大数据是指在海量数据中提取、分析和利用信息的过程，而信息通信技术是收集、传送、存储、处理和展现信息的一系列技术。在当今社会，大数据和信息通信技术已经成为紧密联系的两个领域，相互依存，互相促进。

首先，大数据和信息通信技术都是信息时代中的重要组成部分。信息技术的发展促进了数据的产生和积累，而大数据则为信息加以利用。大数据作为信息时代的发展趋势之一，引导了信息技术的不断进步和完善。这种相互促进不断地推动着社会的发展。其次，大数据和信息通信技术的使用为企业和组织提供了更加精准和高效的数据处理和处理能力。大数据提供了更全面准确的数据，而信息通信技术则提供了高效和便捷的数据收集和传输方式。二者的结合可以实现难以想象的优势，为企业和组织提供更加全面、高效和优质的数据应用服务。再次，大数据和信息通信技术的结合可以产生创新性的可持续发展的商业模式。随着大数据技术的发展，人们可以提取和分析海量数据，并针对客户需求制定个性化战略。信息通信技术的使用可以加速这一过程，提高工作效率，缩短反应时间，开拓新客户和市场，提高营销收益和企业利润。不过，大数据和信息通信技术的结合也存在着一些风险问题。由于可能涉及个人隐私，因此必须保证数据的安全和保密。在大数据的加工和利用过程中，存在未经授权访问、数据泄露等违规行为，这些问题需要得到重视和解决。此外，不断进步的人工智能技术也可能会威胁到人类的安全和隐私[1]。

总之，大数据和信息通信技术的结合是信息时代的趋势和未来的发展方向。随着技术的不断进步，我们预计两者之间的融合会变得更加紧密和有效。

2 隐私保护的重要性

隐私保护涉及到保护个人的信息和权益，是信息时代中的重要话题。个人隐私数据通常包括姓名、地址、电话号码、生日以及各种账户信息等。这些数据被滥用或泄露可能会导致严重的后果，如金融损失、身份盗窃、诈骗，甚至会是生命安全风险。因此，隐私保护显得尤为重要。

首先，个人信息泄露会给个体带来巨大的经济损失。随着互联网技术的发展和普及，以及金融和电子商务的兴起，人们的个人隐私数据不断被收集和利用。如果这些个人信息数据不得善意维护，有人利用这些信息进行欺诈或其他不法活动，受害人可能遭受金融损失、不必要的经济负担或造成财产损失和个人隐私泄露。其次，个人资料泄露会导致身份盗窃和其它不法活动。一旦个人信息被盗，犯罪者可能会用假身份提交假冒贷款、信用卡申请等，或者在互联网上注册黑市账户，或者在其他人的名字下进行金融交易等活动，最终导致受害人信用信誉受损。此外，犯罪分子可能会利用个人信息进行网络诈骗和垃圾信息骚扰。通过集聚个人信息，这些犯罪活动者可以收集更多的个人信息以诱骗受害者和客户。随着用户意识的抬头和监管完善，网络诈骗和信息骚扰活动在不断上升，严重威胁到社会的稳定和人民的福祉。最后，不良的数据使用可能会对人们的生命

安全产生影响。综上所述，保护个人隐私数据和信息是重要的。人类的生命安全和财务大权都依赖至关的个人信息数据保护。因此，需要采取相关的法律和技术手段，以确保个人隐私数据的安全和保密。

3 隐私保护的基本理论

3.1 隐私概念和分类

隐私是指人们在生活和工作中，不想被公开或传播的信息和活动。根据信息和活动的属性、范围、利益，可以将隐私分为以下几类：（1）个人隐私：个人隐私是指涉及个人身份、姓名、地址、电话号码、出生日期、婚姻状况、学历等信息。（2）健康隐私：健康隐私指涉及个人健康状况、医疗保健和药品使用等信息。（3）财务隐私：财务隐私指涉及个人财务信息、财务交易和资产负债等信息。（4）社交隐私：社交隐私是指涉及个人社交网络、邮件、通信、互联网使用记录等信息。（5）宗教隐私：宗教隐私是指涉及个人宗教信仰和习俗等信息。（6）性别隐私：性别隐私指涉及个人性别、性倾向和性偏好等信息。（7）活动隐私：活动隐私是指涉及个人时间表、活动密码、餐厅用餐习惯等信息。（8）法律隐私：法律隐私是指涉及个人官方事务、刑事案件、调查工作等隐私。

隐私的广泛性意味着人们在许多不同的领域和情境中都有不同的在向第三方公司提供和使用自己的数据或信息的可能。人们需要认识到不同分类的隐私，以制定适当的保护行动来保护自己的隐私权。

3.2 隐私保护的法律法规、伦理道德及技术手段

隐私保护需要多方面的手段，其中包括法律法规、伦理道德和技术手段。

3.2.1 法律法规：

1）《中华人民共和国个人信息保护法》：该法规定了个人信息收集、使用、处理、保护的范围和条件，并规定了各方的权利和义务，加强了个人信息的保护。2）《中华人民共和国网络安全法》：该法规定了网络安全的原则、重点、责任等，保护个人隐私和个人信息安全。3）《中华人民共和国民法典》：该法规定了个人隐私权的保护，保护个人形象、声音、名誉等合法权益。

3.2.2 伦理道德：

1）敬业精神：职业道德是每个从事相关工作的人必须遵循的规则。所有与个人隐私相关的工作者都应严格遵守工作规则，维护个人隐私，防止隐私泄露。2）诚信：所有人应该为自己的行为和表达负责。在互联网上，用户需要负责任的发布自己的信息，避免非法收集、使用他人的个人信息。

3.2.3 技术手段：

1）数据加密：对于重要的个人隐私数据，可以采用加密技术以避免不必要泄露。2）安全认证：通过建立网络安全认证系统，可以增强用户的网络信息安全，保护个人隐私不被泄露。3）隐私屏蔽：通过设定权限和安全设置，可以控制自己的隐私数据被哪些人或应用程序看到或访问。4）匿名技术：使用匿名化技术或处理技术，可以保护个人隐私数据，使它们在保护隐私的情况下依然可用[2]。

总之，保护个人隐私是个长期性的工作，需要多方面的合力，法律法规和伦理道德方面都需要做到规定和遵守，同时技术工具也应该不断更新和完善。

4 当前大数据下信息通信技术隐私保护的挑战及应对

当前大数据已经广泛应用于社会各个领域，它的普及深入到我们的生活的方方面面。然而，同时伴随着大数据技术的普及，个人隐私保护也成为了重要的问题。大数据技术的增长让更多的个人数据被收集和共享，这既有利于资源的共享和利用，也带来了对个人隐私的潜在风险。同时，作为一项新兴技术，大数据应用的生态系统多样，很难设置一套适用于各种结构的隐私保护规则，因此如何在大数据技术的应用中保护个人隐私一直是诸多企业和用户所面临的难点。因此，本文将探讨当前大数据下信息通信技术隐私保护面临的主要挑战和应对策略。

4.1 当前大数据下隐私保护面临的挑战

隐私保护是当前大数据应用所面临的重要挑战之一。以下是当前大数据下隐私保护所面临的主要挑战。

（1）数据规模和安全处理。大数据技术最具特点的就是其数据处理规模，传统的隐私保护技术难以胜任如此大的隐私数据保护范围，包括隐私数据采集、存储、传输等过程。大数据的数据形式和数据存储挑战传统的隐私保护技术，因此需要研究新型安全防护技术，来保证大数据的安全处理。（2）数据藏匿技术。隐私数据的藏匿是为了确保隐私数据不受共同使用的过程所影响。当数据种类很多时，需要利用数据藏匿技术，有效地对大数据进行隐私保护。（3）数据隐私共享。在多个机构使用同一组数据时，数据完整性和隐私保护是一个重要的问题。虽然目前有一些隐私保护技术可以使用，但仍然存在着许多风险和隐患。（4）保障合法性。在大数据应用过程中，必须保障数据的合法性和合规性。合适的隐私和数据保护法规和政策的实施可以保护隐私数据的合法性和合规性。（5）认证机制。在安全系统中，多种认证方式可以保障数据在第三方机构间的安全传递，认

证机制也应能满足第三方机构的安全要求。

4.2 大数据下隐私保护的应对策略

（1）建立隐私体系。在大数据应用中，建立起符合各个行业特点和需求的对隐私保护的体系框架是很有必要的。隐私保护系统应该在多方面考虑，始终保证隐私保护规则的透明化。（2）数据匿名处理。保障数据的隐私和安全是重要的，但数据需要依然能够被合理运用。因此，在数据收集和存储过程中采用数据匿名技术来保护隐私。（3）数据加密技术。数据隐私的加密技术是一种重要的数据保护措施，应用于大数据的数据加密技术能够对数据进行保护，但同时需要考虑加密算法的适应性和技术成本。（4）数据授权管理。数据隐私保护不仅体现在数据收集、存储和处理过程中，也需要考虑数据的使用问题。建立一个削减数据使用风险隐私保护的规定，要求在合理授权的前提下使用数据、对数据使用后进行监控，保障数据被使用时的安全性和完整性。（5）保证数据合法性。保证数据的合法性和合规性对于大数据隐私保护至关重要。制定更为严格和规范的数据保护法规和政策，保护隐私数据的合法性和合规性，对于防止恶意用户和企业得到隐私数据，或使用隐私数据来进行违法行为至关重要。（6）数据共享管理策略。数据共享中的数据完整性和隐私保护是一个重要的问题，制定数据共享管理策略，确保涉及隐私的数据难以自动访问或手动访问。更新合适的访问政策，保障数据共享和隐私保护成果有效，为前二者提供重要的组成部分[3]。

5 未来研究方向和发展趋势

大数据下信息通信技术的隐私保护是一个长期和紧迫的问题。为了更好地保护个人隐私，就需要在大数据和信息通信技术领域开展相关的研究。未来，大数据下信息通信技术隐私保护的研究方向和发展趋势可能包括以下几个方面：

5.1 基于AI和机器学习的隐私保护技术

人工智能和机器学习是当今最流行和最热门的技术，可以在不影响数据的使用的同时提高大数据隐私保护的能力。通过对隐私数据进行加密、脱敏和分割等处理方式，进一步保证隐私数据在共享过程中的安全与可控。

5.2 基于区块链的隐私保护技术

应用区块链在隐私保护方面,可以确保数据采集、存储和共享过程中数据安全可靠，由于区块链的不可篡改性和去中心化的特点，能够有效的限制恶意越权行为的发生，保护用户数据，防止恶意利用泄露用户隐私的问题。

5.3 隐私安全计算技术

隐私安全计算技术是一种新的控制类隐私保护技术，该技术常用于数据库隐私保护、云计算数据隐私和计算资源隐私保证。在保护隐私的同时，实现多方参与计算和协同工作，有效地支持数据共享和数据利用。

5.4 端到端的隐私保护机制

端到端的隐私保护机制是保障用户隐私的一项重要技术，通过端到端的方式对数据进行加密保护，防止数据被其他用户访问或泄露，更加安全可靠。同时，端到端的技术方案是可以与秘钥管理方案进行配合，加强秘钥管理的可信度，实现数据安全和隐私保护的完整性。

5.5 面向智能合约的隐私保护技术

智能合约是区块链技术的核心，是一种自动执行的合约模式。结合大数据应用和区块链技术，将智能合约作为控制节点，通过加密和授权方式保护隐私保护，从而实现可控的数据共享。

这些新技术的研究和应用，会为大数据隐私保护带来新的突破和进展。因此，我们应该持续关注和积极研究新的隐私保护技术，努力打造一个安全、稳定和可信赖的大数据应用生态系统。

结语

在大数据应用领域，隐私保护问题是一个全面、复杂和跨学科的问题。很多人和组织都认为现有的技术和政策不能满足日益增长的隐私保护需求，需要重新规划、开创和创新的方法。为此，建立和完善的隐私保护系统，开发先进和可调整的隐私保护技术，以及确保数据隐私的合法性和合规性，成为大数据应用下隐私保护的重要目标。通过我们各方面的努力，大数据的应用才有望取得成功，推动大数据技术的发展和应用，同时也保护了每个人的隐私安全。

参考文献

[1]张涛,肖伟.大数据时代隐私保护技术研究与应用[J].计算机科学,2018,45(7):17-21.

[2]施嘉鹏,赵瑞,康雅萍.大数据隐私保护技术研究综述[J].现代计算机,2017(6):13-17.

[3]邓兆芳,张哲,王岸洲.大数据隐私保护研究进展与挑战[J].网络与信息安全学报,2019,5(3):96-108.