“数码社会”的安全 – 新的风险和风险管理

1. 导言

首先大体介绍一下数码社会出现的几种新的风险，然后概括一下对付这些风险的有可能使用的一些方法。“数码社会”是指在一定社会中，个人和组织利用信息技术进行日常工作和消遣，并通过数码网络与其他个人和组织进行交流。 *新的风险*

对付风险，其效果只可能达到减少损失发生几率和数量。风险的特性决定了它不可能完全杜绝，我们所说的“风险管理”一词，是用来形容不断出现的风险。 *风险管理*

对某一种风险类型进行解释后，本文会描述一到两种对付这类风险的方法。报告的重点，是国家管理风险的方法。数码社会中，私营企业被越来越多地要求直接解决风险问题，它们也一直在积极地采取技术上的和组织上的方法，解决问题。但国家需要作出表率，明确支持什么，反对什么。对普遍存在的问题，要为社会整体出力解决。 *国家作用*

范例都引用德国的。必须记住，德国的方法已植入欧盟的方法之中。在必要的时候，会引用一些欧盟的做法。 *全球含义*

最后要说的一点是，数码社会无国界。德国的方法即便是被欧盟采纳的，同时也可作为全球解决问题的方法。上周在日内瓦召开的网络安全（注释 1）专题研讨会上，大家再次对此话题进行了讨论。这个会议是为今年九月在突尼斯召开的信息社会世界峰会做第二部分的准备。我荣幸地主持了关于安全和数据保护之间关系的讨论会。本报告将涉及这一议题。

全球含义

2. 新风险

数码社会的风险类别

报告将集中讨论数码社会风险的典型类型。风险有很多种分类方法，可根据动机、手段，或价值所受到的侵害进行分类。报告选择中性的方法予以分类，既数码社会有三个层面面临风险，一是依赖网络的总体基础结构，二是通讯关系，三是信息。我们可以根据这三方面对风险类别加以归纳：

新风险

- 基础结构风险；
- 通讯风险；
- 信息风险;

2.1.1 基础结构风险

基本结构风险，是指部分或全部地，暂时、一段时期或长时期内，总体通讯基础结构瘫痪。这种风险的发生，不仅由于数码结构的威胁造成的，还可能由支持数码基础结构的各组成部分引起。这类风险通常称为国家风险。

结构风险

2.1.2 通讯风险

“通讯风险”发生在社会交流的中、小范围内。这类风险，尽管不能说是绝对的，但基本上是影响到了公共或私有部门企业之间，个人之间以及个人与组织之间的通讯过程。数码社会，对通讯工具的设计，主要是力求简便，而不是保障其安全性。因此，通讯系统的设计偏重于公开准入。

通讯风险

没有装备安全措施，并非遗漏，而是本来就认为可有可无，只是在特殊需要时，才加以安装。数码技术的使用者，已经习惯于系统缺陷，网上交流时，并不防备不受欢迎的入侵者、偷听者，或是冒名顶替，以假身份进入网络交流的人。

注释 1 ： http://www.itu.int/osg/spu/cybersecurity/index.phtml.

2.1.3 信息风险

最后一类是信息风险，是指信息内容和经过数码处理的信息文字所面临的危险，例如未经授权进行破坏、改变或窃取、伪造信息，以及制作断章取义的信息等。

信息风险

特别是信息风险，可能在数码通讯网络外部发生。比如一封信被偷了，一张报纸登载了与某人不符的消息等。这类风险之所以成为数码社会的典型风险，是由于新环境下“传统”风险的范围改变了。在一份乡间报纸上登错了某人的信息，和在互联网上登错了信息，其含义自然是不一样的。

信息风险作为 IS 风险

这个例子将我们引入了数码社会中更为普遍存在的风险。这种风险可以把所有“过时”的风险都变成数码社会中“时尚”的典型的风险。

2.2 数码社会存在的普遍风险：不对称效应

我们可以借用结构风险的例子来解释“不对称效应”的含义。

有个十八岁的德国人，上星期刚被德国法庭判了刑，原因是他释放的电脑病毒，更准确地说是一种蠕虫，叫做“萨斯尔病毒”,导致一年前全世界电脑系统的瘫痪。这个年轻人的行为，受到了有关刑法的制裁，这个刑法，是几年前制定的。也就是说，相应的刑法系统已经建立起来了，但安全措施却没有跟上去，人们还是习惯于打开每一个发给他们的邮件。

这里，更重要的是，怎么凭借他单个人的力量，就可以制造出如此巨大的后果，大部分的网络基础结构都停止运转了。在高度依赖技术结构的社会里，可以不费吹灰之力，造成巨大影响。这种不对称的易受攻击性，不仅在数码社会很普遍，对任何依赖技术运转的社会，都是如此。信息和通讯技术的高度自动化，扩大和加速了这种“不对称效应”。

小动作后果严重

不对称性产生不良后果，这就要求社会对风险加以管理。在预防风险，防止这类突然袭击发生的可能性方面，所需资源，远远大于制造一次导致严重后果的突然袭击所需要的资源。

然而，数码社会的“不对称效应”还存在另外一个更隐密的效应，本身就可能产生风险。既然微小的动作可以造成巨大的后果，加之预防风险所需资源远远大于制造风险所需资源，人们就可能失去对风险管理的应有认识。

不对称反应

“不对称反应”这一课题，是目前知识产权领域的争论焦点。现在，人们凭借新科技，可以毫不费力地生产和发行高质量的复制品，和过去制作原件所花费的工夫无法相比。知识产权和创新领域，也存在“不对称风险”现象，立法机构对此做出了反应，但是，这种反应也被认为是很“不对称”的，妨碍了新概念和新发明的推广。

3. 数码社会的风险管理

为更好地理解后面谈到的具体事例，首先要介绍一下风险管理的三个主要方面:

- 在很大程度上，数码社会的风险管理与传统社会的风险管理，并不存在很大差别。简单地了解一下数码社会的法律（看以下 3.1），就清楚了。
- 数码社会的风险管理，也产生某些具体问题，这些问题对数码社会来讲，相当典型。讨论“风险控制的矛盾”概念时（以下 3.2），会讨论这个问题。
- 最后，由于本报告的重点是国家风险管理，有必要简单地介绍一下国家干预的几种特别情况(3.3)。

3.1 传统方法：例如采取法律手段

法律手段

数码社会的风险管理方法，在很多情况下，类似于传统社会中的风险管理。通过采取组织的、金融的和心理的手段，预防风险的发生。对风险做出核心反应的，应该是法律。法律是风险管理所依赖的机制：

刑法

- 例如刑法。刑法谋求制定出一套威慑制度，当威慑无效时，则采取惩罚措施；

私法

- 私法建立了一套行为规范制度，或由有关群体通过合同建立行为规范制度的框架。当私法条文执行不利，法律则设立赔偿条例;

赔偿法

- 一项高度复杂的法律分支细则系统，有约定义务之外的赔偿法。赔偿法就未被履行的义务，规定了责任承担和补偿条款。赔偿法，产生的结果，很是耐人寻味：一方是责任方，他们竭尽全力，不让自己承担资金赔偿；而另一方是保险公司，他们可从保险金额和因未履行义务而罚款的金额数量之间找到对其有利的关系，从中得到好处。保险公司为了“优化”这种关系，往往设置“前期控制”性措施，强加于被保险方。保险公司威胁说，如“前期控制”措施没有到位，保险公司不负赔偿责任。从这个意义上讲，保险公司对提高安全水平，还真是作出了贡献。

3.2 数码社会风险管理的具体特征：风险控制自相矛盾

在数码社会，风险管理有一个突出的特征，叫做“风险控制的自相矛盾”，它引起了公众对数码社会的效应和风险的许多辩论。

我们借用通讯风险的范例来解释“风险控制自相矛盾”的含意。

通讯风险的范例

从以上阐述中，大家都已看到，网络的准入设计引来了恶意袭击。网络结构促进了开放式的网络准入，使信息得以传送。但网络并不设计指定的信息路线，网络上的每一条信息，都应提供来源和地址。网络路游器必须对这部分信息进行贮存，才能引导整套信息通过网络。在对抗开放式结构带来的风险时，可利用信息,追踪恶意攻击的策划者。

换句话说，数码技术的特征在于，一方面它制造风险，另一方面也为对抗风险提供了机制。但这只是第一层面的问题。

第一层面

第二层面

“风险控制的自相矛盾”还有进一步的含义：通过技术构建的风险管理机制，反过来也会制造风险。举例来说，加强网络监控，不仅影响了网络的运行性能，同时还大量收集监控到的信息，这就带来滥用信息的新的潜在风险。持续不断的监控，使公开讨论很别扭，而公开讨论是合法性和权利的基础。.

3.3 国家管理风险的具体特征

本报告的重点是，国家通过政府和立法机构进行风险管理的手段。

国家管理风险

这并不等于说，只有国家才对风险管理负有责任。恰恰相反，公民和私有企业也须承担起管理他们自己风险范畴的责任。私有部门之间应相互交流经验，利用彼此的产品和服务，改善风险管理，加强对员工个人的培训。

风险管理的责任

当然，国家肩负的责任更大，手段更多。国家承担对内对外安全的责任，有必要采取措施，提高公共部门的安全。国家可通过对公共部门与私有企业的协作合同，制定标准，以此对私有企业的安全水平施加影响。

法制国家准则

国家的一切行动，必须以“法治国家”作为准则。“法制国家”的概念包括若干原则。我们所谓的“法治国家”， 要求一切国家行动，以法律为准绳。法律赋予国家执行行动的效力，同时也对其行动设置限度。法律规定国家可以在多大程度上干涉公民的个人权利。公民也有可能对国家的干涉，向法庭上诉。法庭就要努力均衡有关双方的利益。这些法律准则同样适用于安全措施。所有安全措施所具备的条件限制，应不与“法制国家”的观念相左。当然，安全问题的重要性，会对法庭如何均衡双方利益产生影响。

本文中，“法治国家”一词要求，国家无论在任何时候，采用任何风险管理的手段，无论是组织上的、金融上的，还是技术方面的手段，都必须以法律为准绳，或至少必须具备法律授权的明显联系。

以国家权力机构对抗安全风险为依据，许多法律已经出台。数码社会同时提出了问题，在多大程度上，需要出台新的法律。报告还将列举一些实例。

由国家机关运做的法律系统，有时候会出现节奏慢、效率低的现象，官僚主义障碍重重。特别是在发生迅速而深刻的技术和社会变革的时候, 虽然酝酿着各种各样的解决方法，但显而易见，变革不能没有法律。要有允许更多灵活性的法律，鼓励公有和私有部门之间合作的法律。不能当公民感到他们的权利受到威胁的时候，逃避责任，不给公民在法庭上讨回公道的机会。

4. 数码社会的风险管理 – 事例

对第二部分归纳的每一种风险类型，下文至少对它的一种措施予以详尽描述。

在对抗基础结构风险的措施方面，以德国联邦信息安全办公厅为例。将对它的设立、作用和功能进行描述。 *基础结构风险*

通讯风险方面，将介绍两种解决途径: *通讯风险*

- 数码签字方法：建立一个全国性的基础结构，用于安全和身份识别，对抗信息通讯中存在的一些风险。 *数码签字*
- 第二种方法：是数据保留方法，这种方法也可作为数码社会风险控制矛盾的范例。数据保留方法，是用信息技术对抗信息技术风险。同时，这同时是风险管理方法再次制造新的风险的例子。对这种方法，还需进行社会性探讨。 *数据保留*

最后的例子，介绍一套法律手段，降低信息内容、质量、含义、背景等方面的风险。 *内容*

4.1 基础结构的风险管理 - "BSI"事例

德国，和其它国家一样，已经采取了法律、组织和技术方面的措施，目的是最大限度地降低（德国）信息基础结构的风险。这些措施的实行，成为联邦和地区一级的政府的职能范围，对国家和内部安全所承担的职责。

在欧盟，欧盟理事会部长会议最近通过了一项决议，要求所有成员国协调刑法，目的是对各种级别上可能发生的袭击，形成共同的威慑（注释 2）。

其中之一的措施将予以详尽叙述，即：建立联邦信息安全办公厅，这项措施超越了国家安全的范畴，目的是在整个德国，加强对风险的注意和防范。 *联邦信息安全厅*

1990 年，建立了联邦信息安全厅（简称 BSI）(注释 3），属于联邦内务部的特别机构。

联邦信息安全厅(注释 3)：

- 向德国政府提供中央信息技术服务，就政府各部的信息防务问题提出建议和支持； *服务/支持*
- 进行研究，组织研讨会，讨论信息安全问题，大多数讨论结果向公众公开； *研究*
- 为各级公共行政单位制造信息安全软件，准则，组织手册；采取步骤，向公众进行信息安全教育。 *产品 提供服务*

注释 2　理事会框架决定 2005/222/JHA，2005 年 2 月 24 日
注释 3　http://www.bsi.de

仅互联网一项，BSI 就建立起六个运做单位：

- *电脑应急反应小组（CERT）*：为政府部门设立的解决电脑和网络安全问题的中央协调机构。对从制造商和其他来源的与安全有关的信息加以分析，评估和加工，交给目标（任务）小组。服务机构开动信息邮件系统，向使用者团体报警。 在制造商的协助下，为解决安全风险，提供合适的措施。该办公厅下，设有应急小组，可对特殊情况进行干预;
- *互联网安全分析和程序处*：负责因特网安全的基本研究。发表办法、程序和工具;
- *向镇压刑事犯罪提供支持处*：中央协调机构，在防止和调查针对信息技术安全的犯罪方面，向镇压刑事犯罪部门提供技术支持;
- *反对破坏计划和电脑病毒处*：提供咨询意见，对付坏码，向用户和制造商提供涉及目前电脑运做系统和实际程序的安全方面的建议;
- *通讯技术渗透中心*：检查公共行政部门的电脑系统存在的弊端，就如何去掉弊端提出建设性意见。必要时，中心可以协助公共行政部门，提供对付袭击的分析和防范办法。
- *关键基础设施处*：检查涉及因特网信息安全的相关关键性基础设施部分。

BSI 年度预算约 4500 万欧元，有 380 名雇员。办公厅在公共和私有部门地位很高，也有些批评意见。办公厅政治上隶属于内政部的政策。

4.2 通讯风险的管理

就这个议题，我介绍两种方法，一是数码署名方法，二是数据保存方法。

4.2.1 数码签字

数码签字一词，经常在讨论电子商务如何推动商业交易时被提到。但它的功能，还不仅停留在电子商务这个范畴里。数码签字的方法，可以用来解决在数码通讯媒体中进行交流时，交流双方不能明确辨别对方身份的问题，还有就是交流的内容可能被其中一方拒收。

数码签字定义

数码签字，起用了一个被称做“公共钥匙加密”的加密方案。每一个参与者得到两把钥匙，一把是保密的，叫做“私人钥匙”，通常安装在电脑的可读卡片上；另一把叫做 “公共钥匙”，这把钥匙对所有人公开，被收录在某一个公共登记处。

举个例子。A 先生想发送一个信息给收件人 B 先生，他用保密钥匙对信息进行了编码，然后发送给了 B 先生。B 先生知道信息是从 A 先生那里发送的，他在某个公共登记处查找了 A 先生的公共钥匙。B 先生使用 A 先生的公共钥匙，破解了这个信息，条件是，这条信息一定是 A 先生发送的。

在实际运用中，这个步骤被用来在电子系统中签定合同。合同的签定还需要加入另外一个技术步骤，即用数学方法，制造一个文本“手印”。手印是为文本特意制作的，也只用于文本本身。只要原始手印出现任何微小的变动，都会变成另一个“手印”。

在刚才的例子中，A 先生将合同和手印一同发送给了 B 先生，A 先生没有对合同加密，但他用保密钥匙对合同的手印进行了加密。B 先生收到 A 先生的合同，也为他自己制造了一个合同里的手印。然后 B 先生查找 A 先生的公共钥匙，并用它对 A 先生合同上的手印进行解密。如果从 A 先生那里得到的被解密的手印，和 B 先生自己制造的手印相吻合，那么 B 先生就会知道：

- 原文是 A 先生发送的，并且只能是 A 先生；
- 合同文本在 A 加密了手印后，没有被改变过。

全国范围的识别系统

为在全国推广，必须有一个可以信赖的机构。只有接受方在这个机构中确认了他们的身份，才会发放这两把钥匙。另一个例子是竞争公司发放这两把钥匙，但必须获得某个中心权利机构的认证，以确保运行符合标准和安全。这种方法，欧盟在 1999 年(注释 4)有关电子签字的指令中就已提出来了。

德国事例

在此框架之下，德国建立了一个中央权力机构，对其它权利机构或公司(注释 5)进行认证，这个机构叫邮电及通讯管理局，现在它掌管着 15 家以上的服务公司。德国法律改变了对纸张文件上正规签字的正式质量要求。凡符合法律（注释 6）要求的合同，都可以在全国更广范围内使用新的系统。

尽管如此，这种方法没有在德国广泛使用开来。它的使用还只限于法律业内，律师用它进行相互间交流，和法庭进行联络等。使用群体的数量有限，例如税务会计。

为了鼓励数码签名方法在全国推广，已经有人建议，除了给出两把钥匙，同时还给出一张国家身份证(注释 7)。

4.2.2 数据保留

概念

“数据保留”是指通讯服务商，包括网络服务商，有义务对网络上的活动情况进行记录，以用来辨别某一特定时间内的每一位用户的身份，并在执法机关要求查看时，随时提供记录的信息。

德国事例

德国目前没有对数据保存规定义务的法律。

根据 2004 年 6 月版的德国电讯法和它的有关规定，服务商有义务和执法机关共享实时网络活动情况和内容。 执法部门,在被授予恰当权利情况下，可以：

- 要求信息服务商寄给执法部门目前网上活动情况的原始记录；
- 要求信息服务商提供储存的信息记录，例如给客户的结算单等.

注释 4 http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf
注释 5 2001 年 5 月 16 日通过的电子签字法
注释 6 参阅 1999 年中华人民共和国合同法第 11 条
注释 7 http://www.br-online.de/wissen-bildung/thema/egov/signatur.xml 报(德语网站)

但执法机构不能够要求信息服务商储存信息。

信息服务商是否储存信息，取决于他们与客户签定的合同的条款和管理客户的方式。服务商可以储存什么样的信息，储存多久，在德国电讯法的数据保护部分进行了规定。根据规定，服务商对信息的最长储存时间是六个月。德国最大的互联网服务商，“t-在线”，目前对用户活动信息的储存是八个月。就在上周，德国法庭宣布 t-在线的这种做法是违法行为（注释 8）。

欧盟和目前的讨论议题

欧盟通过部长会议已经进行了多次努力，规范各成员国制定的法规，以便要求各成员国对数据进行储存。

2005 年 1 月，德国议会要求德国政府继续执行现有的法律规定，最长储存时间为六个月。

就在上个月，欧洲议会没有通过部长会议的提议。提议在九月份还会重新讨论。

反对意见

反对数据保存，部分原因是出于对费用的考虑，储存信息要求通讯服务商支付费用。反对贮存的争论焦点是，和所能达到的目的相比，投入过高；另外还有一点，就是它触及了隐私法，在一定程度上，得不到充分的论证。

4.3 信息风险管理 - 数据保护

内容和正文的风险

信息管理，包含对信息进行了错误管理而产生的风险。对个人信息进行了错误处理，会触及公民的隐私权。这些危险在数码社会之前也发生过，就是我之前介绍过的“不对称效应”。对个人信息进行电子化管理时，需要利用新的方法来对付风险。信息保护法解决了该问题。数据保护法一词是从历史演绎出来的，具有误导性。得到保护的，应是个人信息的隐私性、完整性和自由，打击一切不正当使用信息的行为。

德国事例

德国的数据保护法，在各省和联邦机构都已实施，它对所有公共部门和私有企业都适用。对于具体行业，制定了特殊的隐私法，例如刚才谈到的电讯行业。德国的数据保护法符合欧盟 1995 年通过的数据保护法令(注释 9)。

制定数据保护法的主要原则可归纳如下：

- 对收集和处理个人信息进行立法，必须具备法律理由。这种法律理由，可以是一项法律，允许对个人数据、合同加以处理，或是得到了有关方的同意，也可以是在特殊情况下，存在优先于个人利益或公共利益的理由;
- 收集和处理的信息，必须正确，不断更新。信息量不应该过大，或是因为收集是合法的，就去收集;

注释 8　查看判决内容,网址: http://www.jur-abc.de/de/ip.htm.
注释 9　了解更多欧盟数据保护状况, 网址: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

- 收集或处理的数据，除某些特殊情况，当事人有权了解；如数据有假，可以要求更正；如果数据是通过违法途径收集，则当事人可以要求销毁;
- 设立独立的权利机构，教育公共和私有部门如何对个人数据进行管理。数据保护规定同时监督公共和私有部门对个人数据的管理情况。

难度

在实践中，管理个人数据的法规，遇到了诸多困难，特别是在互联网时代。这些法规适用于互联网，是因为大部分条文的制定，采用的是中性技术，而实际问题则复杂得多。举例来说，互联网的用户，必须了解，他们点击网页的活动怎样受到本国或外国公司出于广告的目的进行的监控; 还有的用户，必须明白自己的电子邮件地址怎样会落入他人手里，造成邮箱里垃圾邮件泛滥成灾。

国家法律的局限性

如果各国政府都能保障公民的权利，（欧盟内）其他政府也会协助保护公民权利，只有这样，制定国家数据保护法才算真正有意义。欧盟内部，通过数据保护条令，各国达到了共识，制定了成员国数据保护的水准。欧盟也可以和第三国达成协议，推动个人信息向它国转移，前提是这些国家已经立法，规章制度可以和欧盟相比。欧盟已经和某些第三国签署了协议。

最后，还应注意到，早在 1990 年，联合国大会就向其成员国(注释 10)推荐了数据保护指导方针。

5. 结论

对于目前数码社会存在的诸多风险，我着重解释了其中三种：影响国家信息结构的风险；影响组织和个人通讯的风险；对信息本身产生影响的风险。

我还描述了它们两个与数码社会有密切联系的总体特征，一是起因和效果之间的不对称效应，二是风险控制的自相矛盾。

对每一种风险，我都列举了几种管理方法，比如建立德国联邦信息安全局，处理基础结构的风险。利用数码署名方案，解决通讯中出现的身份识别问题。在数据保存方法方面，介绍了怎样衡量这种技术解决方法对社会可能造成的影响。 最后，我还介绍了数据保护，如何作为一种机制，消除对信息的质量和内容产生影响的某些风险。

由于时间有限，我只能举出一些例证。尽量引用国家的例证。但我说过，真正的挑战在于寻求国际上都适用的解决方法。

我注意到，本文提到的许多问题，在中国已研究出了解决办法。如电子签名方法（ESA），具我所知，三个月前已经开始使用。还有一些法规，例如艺术界隐私条例。中华人民共和国宪法第 38 条，1998 年制定的中华人民共和国电脑

注释 10　电脑个人信息档案的指导方针 - 联合国大会 1990 年 12 月 14 日 采纳

信息网络与国际连接管理的暂行条例第 18 条，中华人民共和国宪法第 40 条，以及 1997 年制定的电脑信息网络与国际连接的安全保障和管理实施办法的第 7 条等。

希望能了解更多的解决方法。

*作者：赫尔波特·波克特

公共法律、信息和通讯法教授；瑞士圣加仑大学信息法研究中心主任；德国圣奥古斯丁市佛兰豪夫媒体通讯研究所研究员