

一种基于隐私保护的数据风险防控方法、装置及设备

技术领域

[01] 本说明书涉及计算机技术领域，尤其涉及一种基于隐私保护的数据风险防控方法、装置及设备。

背景技术

[02] 随着互联网的快速发展，以及互联网对用户生活渗透的深度不断加深，隐私保护越来越受到重视。在用户敏感信息（如隐私数据）保护的场景中，存在一个核心的问题，即用户的隐私数据不会与货币一样，因为货币是可以被消耗的，并且也可以被追溯，而用户的隐私数据是可以无限次被拷贝和被流转的，从而导致用户隐私保护相对货币的保护更加困难，为此，需要提供一种能够对用户隐私数据的生产、流转、拷贝、销毁等处理过程进行管控的技术方案，以实现用户对用户隐私的保护。

发明内容

[03] 本说明书实施例的目的是提供一种能够对用户隐私数据的生产、流转、拷贝、销毁等处理过程进行管控的技术方案，以实现用户对用户隐私的保护。

[04] 为了实现上述技术方案，本说明书实施例是这样实现的。

[05] 本说明书实施例提供一种基于隐私保护的数据风险防控方法，所述方法包括：获取目标隐私数据的处理请求。确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息。基于所述目标隐私数据对应的隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建。在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

[06] 本说明书实施例提供一种基于隐私保护的数据风险防控装置，所述装置包括：请求获取模块，获取目标隐私数据的处理请求。属性获取模块，确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息。管控规则确定模块，基于所述目标隐私数据对应的隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建。管控模块，在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

[07] 本说明书实施例提供一种基于隐私保护的数据风险防控设备，包括处理器以及被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：获取目标隐私数据的处理请求。确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息。基于所述目标隐私数据对应的隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建。在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

[08] 本说明书实施例还提供了一种存储介质，其中，所述存储介质用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：获取目标隐私数据的处理请求。确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息。基于所述目标隐私数据对应的

隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建。在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

附图说明

[09]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[10]图1为本说明书一种基于隐私保护的数据风险防控方法实施例；

[11]图2为本说明书另一种基于隐私保护的数据风险防控方法实施例；

[12]图3为本说明书一种隐私保护过程和隐私保护切面的示意图；

[13]图4为本说明书一种基于隐私保护的数据风险防控装置实施例；

[14]图5为本说明书一种基于隐私保护的数据风险防控设备实施例。

具体实施方式

[15]本说明书实施例提供一种基于隐私保护的数据风险防控方法、装置及设备。

[16]为了使本技术领域的人员更好地理解本说明书中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本说明书保护的范围。

实施例一

[17]如图1所示，本说明书实施例提供一种基于隐私保护的数据风险防控方法，该方法的执行主体可以为服务器或终端设备，其中，该终端设备可以如笔记本电脑或台式电脑等计算机设备，还可以如手机或平板电脑等移动终端设备。该服务器可以是某项业务（如进行交易的业务或金融业务等）或需要对隐私数据的使用过程进行风险防控或管控的服务器，具体如，该服务器可以是支付业务的服务器，也可以是与金融或即时通讯等相关业务的服务器等。本实施例中的执行主体以终端设备为例进行说明，对于执行主体为服务器的情况，可以参见下述相关内容，在此不再赘述。该方法具体可以包括以下步骤：在步骤S102中，获取目标隐私数据的处理请求。

[18]其中，目标隐私数据可以是任意的隐私数据，隐私数据可以是用户不想被其他人在未授权的情况下获取的私密数据，目标隐私数据具体可以如用户的面部图像的数据、用户的指纹数据或用户的身份信息等，具体可以根据实际情况设定，本说明书实施例对此不做限定。处理请求可以包括多种，例如对目标隐私数据进行拷贝的处理请求，对目标隐私数据进行输出的处理请求，生成目标隐私数据的处理请求，对目标隐私数据进行注销或销毁的处理请求等，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[19]在实施中，随着互联网的快速发展，以及互联网对用户生活渗透的深度不断加深，隐私保护越来越受到重视。在用户敏感信息（如隐私数据）保护的场景中，存在一个核心的问题，即用户的隐私数据不会与货币一样，因为货币是可以被消耗的，并且也可以被追溯，而用户的隐私数据是可以无限次被拷贝和被流转的，从而导致用户隐私保护相比对货币的保护更加困难，为此，需要提供一种能够对用户隐私数据的生产、流转、拷贝、销毁等处理过程进行管控的技术方案，以实现用户对用户隐私的保护。基于此，本说明

书实施例提供一种可实现的技术方案，具体可以包括以下内容：为了提高终端设备和各个业务处理的安全性，终端设备中通常会加入用户的身份验证机制，在实际应用中，身份验证机制可以包括多种，例如基于指纹识别的身份验证机制、基于面部识别的身份验证机制、基于虹膜识别的身份验证机制、基于掌纹识别的身份验证机制等，但是不论是哪一种身份验证机制均涉及到用户的隐私数据（即用户的指纹数据、用户的面部数据、用户的虹膜数据或用户的掌纹数据等）。

[20]终端设备中可以安装有某应用程序，通过该应用程序，用户可以进行各种业务处理，在进行业务处理的过程中，为了保护用户业务处理的安全性，通常需要对用户进行身份验证，而身份验证过程涉及用户的隐私数据，由于用户的隐私数据是可以无限次被拷贝和被流转的，因此，如何对用户隐私数据的生产、流转、拷贝、销毁等处理过程进行管控成为需要解决的重要问题。在实际应用中，可以对用于对用户的隐私数据进行处理的各种接口进行改造（或者对用于对用户的隐私数据进行处理的各种接口进行 HOOK 处理），从而可以在上述接口设置隐私数据的风险防控机制，这样，通过对上述接口是否被调用进行检测，从而实现对用户隐私数据的使用过程进行管控，具体地，当终端设备运行上述应用程序时，终端设备可以运行上述隐私数据的风险防控机制，当该应用程序或终端设备在运行的过程中，需要调用用户的某隐私数据（即目标隐私数据）执行某种处理时，可以向终端设备中用于执行该处理的接口发送目标隐私数据的处理请求，此时，终端设备可以检测到上述接口被调用，并可以拦截该目标隐私数据的处理请求，从而可以获取目标隐私数据的处理请求。

[21]需要说明的是，上述应用程序可以为搭载在宿主程序中的小程序，或者，该应用程序也可以为上述宿主程序，该宿主程序可以是移动终端设备或 PC 中安装的 APP 或 IoT 上的应用程序等，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[22]在步骤 S104 中，确定目标隐私数据对应的隐私数据属性信息，该隐私数据属性信息包括对目标隐私数据的使用进行管控所需的一个或多个维度的信息。

[23]其中，隐私数据属性信息可以包括目标隐私数据所固有的属性信息，例如目标隐私数据所属的数据类型（具体如指纹数据类、面部数据类、位置信息类等）、目标隐私数据的创建方信息、目标隐私数据的创建时间和历史访问记录等，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[24]在实施中，通过上述方式获取到目标隐私数据的处理请求后，可以获取目标隐私数据的相关信息，例如，可以获取目标隐私数据的标识，并可以基于目标隐私数据的标识确定对目标隐私数据的使用进行管控所需的隐私数据属性信息，例如目标隐私数据所属的数据类型和目标隐私数据的归属方信息等，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[25]在步骤 S106 中，基于目标隐私数据对应的隐私数据属性信息，确定目标隐私数据所对应的管控规则，目标隐私数据所对应的管控规则为基于专家知识库构建。

[26]其中，管控规则可以包括多种，不同的隐私数据可以设置有不同的管控规则，管控规则中可以包括多个维度对应的规则，例如隐私数据的生命周期维度对应的规则、隐私数据流转行为维度对应的规则、隐私数据的权限维度对应的规则等，具体可以根据实际情况设定，本说明书实施例对此不做限定。专家知识库可以是在实际应用中基于隐私数据的处理经验而得到的知识数据库，也可以是对于隐私数据而随机生成的相关参数构成的知识库等，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[27]在实施中，为了便于对不同隐私数据进行管控，可以针对不同隐私数据设置不同的管控规则，例如对于生物识别类型的隐私数据，相应的管控规则可以为只允许在指定的

有效期内使用，且不允许对该隐私数据进行拷贝操作，具体如，生物识别类型的隐私数据只允许在请求该隐私数据开始计时后的 5 分钟内使用，且不允许对该隐私数据进行拷贝操作，或者，对于属于搭载在宿主程序中的小程序内的隐私数据，相应的管控规则可以为只允许该小程序使用该隐私数据，不允许其它小程序或宿主程序使用该隐私数据，且不允许该隐私数据被流转到其它小程序或宿主程序中等，具体可以根据实际情况设定。

[28]此外，为了简单快速的确定某隐私数据所适用的管控规则，可以根据实际情况，建立隐私数据属性信息与隐私数据的管控规则之间的对应关系，可以如表 1 所示。

表 1

隐私数据属性信息	管控规则
面部识别类型	3 分钟内有效, 不允许面部识别的图像被拷贝, 且不允许面部识别的图像被流转
用户在应用程序中填写的业务信息对应的数据类型	不允许其它应用程序访问, 且不允许流转到其它应用程序中
应用程序获取的用户的位置对应的数据类型	不允许其它应用程序访问, 且不允许流转到其它应用程序中

[29]通过上述方式确定目标隐私数据对应的隐私数据属性信息后，可以基于目标隐私数据对应的隐私数据属性信息，从如上述表 1 所示的隐私数据属性信息与管控规则的对应关系中获取目标隐私数据所对应的管控规则，具体如，目标隐私数据为面部识别类型的隐私数据，则通过上述表 1 可以得到相应的管控规则为：3 分钟内有效，不允许面部识别的图像被拷贝，且不允许面部识别的图像被流转，即用户需要在 3 分钟完成面部识别，同时，在进行面部识别的过程中不允许应用程序或终端设备对面部识别的图像进行拷贝，也不允许将面部识别的图像流转到其它应用程序或终端设备中等。

[30]对于上述步骤 S106 的处理，以上仅是一种可选的处理方式，在实际应用中，上述步骤 S106 的处理可以多种多样，具体可以根据实际情况设定，本说明书实施例对此不做限定。

[31]在步骤 S108 中，在对上述处理请求进行响应的过程中，基于确定的目标隐私数据所对应的管控规则对目标隐私数据的使用合规性进行管控。

[32]在实施中，基于上述步骤 S106 的示例，如果目标隐私数据为面部识别类型的隐私数据（即上述处理请求可以为面部识别请求或支付请求等），相应的管控规则为：3 分钟内有效，不允许面部识别的图像被拷贝，且不允许面部识别的图像被流转，则在对上述处理请求进行响应的过程中（如面部识别的过程中），可以判断用户是否在 3 分钟内完成面部识别，如果否，则拒绝上述处理请求或确定上述处理请求对应的处理失败等，如果是，则同时判断在上述过程中面部识别的图像是否被拷贝，以及面部识别的图像是否被流转等，如果上述处理过程符合该管控规则，则可以完成对上述处理请求的响应，否则，可以确定对上述处理请求的响应失败。

[33]本说明书实施例提供一种基于隐私保护的数据风险防控方法，通过拦截目标隐私数据的处理请求，确定目标隐私数据对应的隐私数据属性信息，该隐私数据属性信息包括对目标隐私数据的使用进行管控所需的一个或多个维度的信息，然后，基于目标隐私数据对应的隐私数据属性信息，确定目标隐私数据所对应的管控规则，目标隐私数据所对应的管控规则为基于专家知识库构建，进而在对该处理请求进行响应的过程中，基于确

定的目标隐私数据所对应的管控规则对目标隐私数据的使用合规性进行管控,从而通过目标隐私数据所对应的管控规则对目标隐私数据的使用过程进行管控,进而能够对用户隐私数据的生产、流转、拷贝、销毁等处理过程进行管控,以实现对用户隐私数据的保护。

实施例二

[34]如图2所示,本说明书实施例提供一种基于隐私保护的数据风险防控方法,该方法的执行主体可以为服务器或终端设备,其中,该终端设备可以如笔记本电脑或台式电脑等计算机设备,还可以如手机或平板电脑等移动终端设备。该服务器可以是某项业务(如进行交易的业务或金融业务等)或需要对隐私数据的使用过程进行风险防控或管控的服务器,具体如,该服务器可以是支付业务的服务器,也可以是与金融或即时通讯等相关业务的服务器等。本实施例中的执行主体以终端设备为例进行说明,对于执行主体为服务器的情况,可以参见下述相关内容,在此不再赘述。该方法具体可以包括以下步骤:在步骤S202中,获取目标隐私数据的相关信息,目标隐私数据的相关信息包括目标隐私数据对应的隐私数据属性信息、目标隐私数据的生命周期信息、目标隐私数据的流转行为信息和目标隐私数据的权限相关信息中的一种或多种。

[35]在实施中,为了制定隐私数据精细化管控的逻辑,可以根据实际情况设定一个或多个不同的维度,例如隐私数据类型维度、隐私数据的归属维度、隐私数据的生命周期维度、隐私数据的流转行为维度和隐私数据的权限维度等,其中,隐私数据类型维度可以包括:位置类、环境类(可以包括终端设备内部的环境和终端设备外部的环境等)、生物识别类(可以包括指纹识别类、面部识别类等)等。隐私数据的生命周期维度可以包括隐私数据的有效时长、流转次数和拷贝次数等。隐私数据的流转行为维度可以包括流转目标、流转方式、流转方向等。隐私数据的权限维度可以包括哪些代码角色可以接触该隐私数据、哪些代码角色可以拷贝该隐私数据、哪些代码角色可以转发该隐私数据、哪些代码角色可以流转该隐私数据等。隐私数据的归属维度可以包括归属于用户、归属于终端设备、归属于当前应用程序(可以为搭载于宿主程序的小程序或该宿主程序等)等。

[36]在步骤S204中,基于目标隐私数据的相关信息,确定目标隐私数据所对应的管控规则。

[37]在实施中,针对隐私数据的精细化信息,制定对应的管控规则,例如,对归属于用户的生物识别信息,对应的管控规则具体可以如只允许存在5分钟,且不允许被拷贝。再例如,对于归属于某小程序的隐私数据,对应的管控规则具体可以如不允许被其他小程序访问,不能允许被流转到其他小程序等。具体可以根据实际情况设定,本说明书实施例对此不做限定。

[38]在步骤S206中,将目标隐私数据加入到需要预设的隐私保护切面进行管控的队列中。

[39]其中,隐私保护切面可以是指针对隐私保护的Aspect,面向切面编程(AOP, Aspect-Oriented Programming),隐私保护切面是通过预编译、运行时动态代理或者注入的方式,实现在不修改源代码的情况下为程序动态添加功能的编程范式。AOP追求的是调用者和被调用者之间的解耦,提供跨模块的功能汇聚。AOP适合解决程序中涉及横切面(cross-cut)的系统功能,该系统功能往往用过程编程或者面向对象编程都难以解决。基于隐私保护切面可以构建相应的切面防御体系,切面防御体系可以是一种安全防御体系,其核心是安全融入架构,可以对代码进行分析和管控,切面防御体系的核心思路是建立一套与业务相交织且平行的安全层,让安全能够深入业务逻辑,实现细致的观测和攻防,同时又保证业务和安全的解耦合,使得业务和安全各自独立。切面防御体系

可以通过安全切面防御层嵌入到了整个应用程序（如 APP）的框架中，同时保持独立运行的规则引擎和升级能力，APP 中包含的重点安全相关的接口可以通过切面进行保护。另外，隐私保护切面或切面防御体系判断某个调用是否合理时，会追溯查看调用的链路信息，对链路的调用风险进行透视，以做出准确全面的判断。

[40]在实施中，可以通过隐私保护切面对目标隐私数据的使用过程进行管控，为此，可以将目标隐私数据加入到需要预设的隐私保护切面进行管控的队列中。

[41]在实际应用中，如图 3 所示，隐私保护切面可以包括隐私保护第一子切面和隐私保护第二子切面，隐私保护第一子切面可以用于在当前终端设备中对目标隐私数据的处理进行管控，隐私保护第二子切面可以用于对从当前终端设备输出目标隐私数据的处理进行管控，基于上述隐私保护切面的分工，上述步骤 S206 的处理可以包括：基于目标隐私数据的处理请求，将目标隐私数据加入到需要隐私保护第一子切面和/或隐私保护第二子切面进行管控的队列中。

[42]在实施中，可以针对任意的隐私数据，预先设定多种不同的处理需求或处理请求，并对于每一种处理需求或处理请求，分别将该隐私数据设定到相应的管控队列中，具体的，如图 3 所示，可以对目标隐私数据的处理请求进行分析，确定该处理请求是否需要将目标隐私数据输出到终端设备之外，如果该处理请求对应的处理不需要将目标隐私数据输出到终端设备之外，则将目标隐私数据加入到需要隐私保护第一子切面进行管控的队列中，如果该处理请求对应的处理需要将目标隐私数据输出到终端设备之外，则将目标隐私数据加入到需要隐私保护第二子切面进行管控的队列中。

[43]在步骤 S208 中，当检测到目标隐私数据的处理接口接收到目标隐私数据的处理请求时，获取目标隐私数据的处理请求。

[44]其中，该处理请求包括目标隐私数据的流转请求、目标隐私数据的拷贝请求、目标隐私数据的采集请求、目标隐私数据的销毁请求和目标隐私数据的消费请求中的一种或多种。

[45]在实施中，当终端设备运行上述应用程序时，终端设备可以运行上述隐私保护切面或切面防御体系，当该应用程序或终端设备在运行的过程中，需要对目标隐私数据进行某种处理时，可以向终端设备中用于处理目标隐私数据的接口发送目标隐私数据的处理请求，此时，终端设备可以检测到上述接口被调用，并可以拦截该目标隐私数据的处理请求，此时，为了保证目标隐私数据的安全性，可以运行预先设定的目标隐私数据的处理请求获取机制，从而获取目标隐私数据的处理请求。

[46]在步骤 S210 中，确定目标隐私数据对应的隐私数据属性信息，该隐私数据属性信息包括对目标隐私数据的使用进行管控所需的一个或多个维度的信息。

[47]其中，该隐私数据属性信息可以包括目标隐私数据的数据类型和/或归属方信息，该数据类型可以包括位置类、环境类和生物识别类。

[48]在实施中，为了制定隐私数据精细化管控的逻辑，可以根据实际情况设定一个或多个不同的维度，例如隐私数据类型维度、隐私数据的归属维度、隐私数据的生命周期维度、隐私数据的流转行为维度和隐私数据的权限维度等。在实际应用中，可以根据实际情况，在上述多个不同的维度中选取一个或多个维度的信息作为目标隐私数据对应的隐私数据属性信息，如可以选取隐私数据类型和/或隐私数据的归属维度的信息作为目标隐私数据对应的隐私数据属性信息。

[49]在步骤 S212 中，基于目标隐私数据对应的隐私数据属性信息，确定目标隐私数据所对应的管控规则，目标隐私数据所对应的管控规则为基于专家知识库构建。

[50] 其中，如图 3 所示，目标隐私数据所对应的管控规则包括目标隐私数据的生命周期的管控子规则、流转行为的管控子规则和权限管控子规则中的一种或多种。其中的生命周期的管控子规则由目标隐私数据的有效时长、流转次数和拷贝次数中的一项或多项维度的信息构建。流转行为的管控子规则由目标隐私数据的流转目标、流转方式和流转方向中的一项或多项维度的信息构建。

[51] 在步骤 S214 中，在对上述处理请求进行响应的过程中，当通过隐私保护第一子切面检测到目标隐私数据被采集和/或被消费时，基于确定的目标隐私数据所对应的管控规则对目标隐私数据的使用合规性进行管控；和/或，在对上述处理请求进行响应的过程中，当通过隐私保护第二子切面检测到目标隐私数据被流转和/或被拷贝时，基于确定的目标隐私数据所对应的管控规则对目标隐私数据的使用合规性进行管控。

[52] 上述步骤 S214 的具体处理可以参见图 3 所示，即当通过隐私保护第一子切面检测到目标隐私数据被消费时，基于确定的目标隐私数据所对应的管控规则对目标隐私数据的使用合规性进行管控；在对上述处理请求进行响应的过程中，当通过隐私保护第二子切面检测到目标隐私数据被流转时，基于确定的目标隐私数据所对应的管控规则对目标隐私数据的使用合规性进行管控。

[53] 本说明书实施例提供一种基于隐私保护的数据风险防控方法，通过拦截目标隐私数据的处理请求，确定目标隐私数据对应的隐私数据属性信息，该隐私数据属性信息包括对目标隐私数据的使用进行管控所需的一个或多个维度的信息，然后，基于目标隐私数据对应的隐私数据属性信息，确定目标隐私数据所对应的管控规则，目标隐私数据所对应的管控规则为基于专家知识库构建，进而在对该处理请求进行响应的过程中，基于确定的目标隐私数据所对应的管控规则对目标隐私数据的使用合规性进行管控，从而通过目标隐私数据所对应的管控规则对目标隐私数据的使用过程进行管控，进而能够对用户隐私数据的生产、流转、拷贝、销毁等处理过程进行管控，以实现用户对用户隐私数据的保护。

实施例三

[54] 以上为本说明书实施例提供的基于隐私保护的数据风险防控方法，基于同样的思路，本说明书实施例还提供一种基于隐私保护的数据风险防控装置，如图 4 所示。

[55] 该基于隐私保护的数据风险防控装置包括：请求获取模块 401、属性获取模块 402、管控规则确定模块 403 和管控模块 404，其中：请求获取模块 401，获取目标隐私数据的处理请求；属性获取模块 402，确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息；管控规则确定模块 403，基于所述目标隐私数据对应的隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建；管控模块 404，在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

[56] 本说明书实施例中，所述装置还包括：队列设置模块，将所述目标隐私数据加入到需要预设的隐私保护切面进行管控的队列中；所述请求获取模块 401，当检测到所述目标隐私数据的处理接口接收到所述目标隐私数据的处理请求时，获取所述目标隐私数据的处理请求。

[57] 本说明书实施例中，所述隐私保护切面包括隐私保护第一子切面和隐私保护第二子切面，所述隐私保护第一子切面用于在当前终端设备中对所述目标隐私数据的处理进行管控，所述隐私保护第二子切面用于对从当前终端设备输出所述目标隐私数据的处理进行管控，所述队列设置模块，基于所述目标隐私数据的处理请求，将所述目标隐私数据

加入到需要所述隐私保护第一子切面和/或所述隐私保护第二子切面进行管控的队列中；所述管控模块 404，在对所述处理请求进行响应的过程中，当通过所述隐私保护第一子切面检测到所述目标隐私数据被采集和/或被消费时，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控；和/或，在对所述处理请求进行响应的过程中，当通过所述隐私保护第二子切面检测到所述目标隐私数据被流转和/或被拷贝时，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

[58] 本说明书实施例中，所述处理请求包括所述目标隐私数据的流转请求、所述目标隐私数据的拷贝请求、所述目标隐私数据的采集请求、所述目标隐私数据的销毁请求和所述目标隐私数据的消费请求中的一种或多种。

[59] 本说明书实施例中，所述隐私数据属性信息包括所述目标隐私数据的数据类型和/或归属方信息，所述数据类型包括位置类、环境类和生物识别类。

[60] 本说明书实施例中，所述目标隐私数据所对应的管控规则包括所述目标隐私数据的生命周期的管控子规则、流转行为的管控子规则和权限管控子规则中的一种或多种。

[61] 本说明书实施例中，所述生命周期的管控子规则由所述目标隐私数据的有效时长、流转次数和拷贝次数中的一项或多项维度的信息构建。

[62] 本说明书实施例中，所述流转行为的管控子规则由所述目标隐私数据的流转目标、流转方式和流转方向中的一项或多项维度的信息构建。

[63] 本说明书实施例中，所述装置还包括：信息获取模块，获取所述目标隐私数据的相关信息，所述目标隐私数据的相关信息包括所述目标隐私数据对应的隐私数据属性信息、所述目标隐私数据的生命周期信息、所述目标隐私数据的流转行为信息和所述目标隐私数据的权限相关信息中的一种或多种；管控规则确定模块，基于所述目标隐私数据的相关信息，确定所述目标隐私数据所对应的管控规则。

[64] 本说明书实施例提供一种基于隐私保护的数据风险防控装置，通过拦截目标隐私数据的处理请求，确定目标隐私数据对应的隐私数据属性信息，该隐私数据属性信息包括对目标隐私数据的使用进行管控所需的一个或多个维度的信息，然后，基于目标隐私数据对应的隐私数据属性信息，确定目标隐私数据所对应的管控规则，目标隐私数据所对应的管控规则为基于专家知识库构建，进而在对该处理请求进行响应的过程中，基于确定的目标隐私数据所对应的管控规则对目标隐私数据的使用合规性进行管控，从而通过目标隐私数据所对应的管控规则对目标隐私数据的使用过程进行管控，进而能够对用户隐私数据的生产、流转、拷贝、销毁等处理过程进行管控，以实现对用户隐私数据的保护。

实施例四

[65] 以上为本说明书实施例提供的基于隐私保护的数据风险防控装置，基于同样的思路，本说明书实施例还提供一种基于隐私保护的数据风险防控设备，如图 5 所示。

[66] 所述基于隐私保护的数据风险防控设备可以为上述实施例提供的终端设备或服务器等。

[67] 基于隐私保护的数据风险防控设备可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上的处理器 501 和存储器 502，存储器 502 中可以存储有一个或一个以上存储应用程序或数据。其中，存储器 502 可以是短暂存储或持久存储。存储在存储器 502 的应用程序可以包括一个或一个以上模块（图示未示出），每个模块可以包括对基于隐私保护的数据风险防控设备中的一系列计算机可执行指令。更进一步地，处理器

501 可以设置为与存储器 502 通信，在基于隐私保护的数据风险防控设备上执行存储器 502 中的一系列计算机可执行指令。基于隐私保护的数据风险防控设备还可以包括一个或一个以上电源 503，一个或一个以上有线或无线网络接口 504，一个或一个以上输入输出接口 505，一个或一个以上键盘 506。

[68] 具体在本实施例中，基于隐私保护的数据风险防控设备包括有存储器，以及一个或一个以上的程序，其中一个或者一个以上程序存储于存储器中，且一个或者一个以上程序可以包括一个或一个以上模块，且每个模块可以包括对基于隐私保护的数据风险防控设备中的一系列计算机可执行指令，且经配置以由一个或者一个以上处理器执行该一个或者一个以上程序包含用于进行以下计算机可执行指令：获取目标隐私数据的处理请求；确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息；基于所述目标隐私数据对应的隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建；在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

[69] 本说明书实施例中，还包括：将所述目标隐私数据加入到需要预设的隐私保护切面进行管控的队列中；所述获取目标隐私数据的处理请求，包括：当检测到所述目标隐私数据的处理接口接收到所述目标隐私数据的处理请求时，获取所述目标隐私数据的处理请求。

[70] 本说明书实施例中，所述隐私保护切面包括隐私保护第一子切面和隐私保护第二子切面，所述隐私保护第一子切面用于在当前终端设备中对所述目标隐私数据的处理进行管控，所述隐私保护第二子切面用于对从当前终端设备输出所述目标隐私数据的处理进行管控，所述将所述目标隐私数据加入到需要预设的隐私保护切面进行管控的队列中，包括：基于所述目标隐私数据的处理请求，将所述目标隐私数据加入到需要所述隐私保护第一子切面和/或所述隐私保护第二子切面进行管控的队列中；所述在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控，包括：在对所述处理请求进行响应的过程中，当通过所述隐私保护第一子切面检测到所述目标隐私数据被采集和/或被消费时，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控；和/或，在对所述处理请求进行响应的过程中，当通过所述隐私保护第二子切面检测到所述目标隐私数据被流转和/或被拷贝时，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

[71] 本说明书实施例中，所述处理请求包括所述目标隐私数据的流转请求、所述目标隐私数据的拷贝请求、所述目标隐私数据的采集请求、所述目标隐私数据的销毁请求和所述目标隐私数据的消费请求中的一种或多种。

[72] 本说明书实施例中，所述隐私数据属性信息包括所述目标隐私数据的数据类型和/或归属方信息，所述数据类型包括位置类、环境类和生物识别类。

[73] 本说明书实施例中，所述目标隐私数据所对应的管控规则包括所述目标隐私数据的生命周期的管控子规则、流转行为的管控子规则和权限管控子规则中的一种或多种。

[74] 本说明书实施例中，所述生命周期的管控子规则由所述目标隐私数据的有效时长、流转次数和拷贝次数中的一项或多项维度的信息构建。

[75] 本说明书实施例中，所述流转行为的管控子规则由所述目标隐私数据的流转目标、流转方式和流转方向中的一项或多项维度的信息构建。

[76] 本说明书实施例中，还包括：获取所述目标隐私数据的相关信息，所述目标隐私数

据的相关信息包括所述目标隐私数据对应的隐私数据属性信息、所述目标隐私数据的生命周期信息、所述目标隐私数据的流转行为信息和所述目标隐私数据的权限相关信息中的一种或多种；基于所述目标隐私数据的相关信息，确定所述目标隐私数据所对应的管控规则。

[77]本说明书实施例提供一种基于隐私保护的数据风险防控设备，通过拦截目标隐私数据的处理请求，确定目标隐私数据对应的隐私数据属性信息，该隐私数据属性信息包括对目标隐私数据的使用进行管控所需的一个或多个维度的信息，然后，基于目标隐私数据对应的隐私数据属性信息，确定目标隐私数据所对应的管控规则，目标隐私数据所对应的管控规则为基于专家知识库构建，进而在对该处理请求进行响应的过程中，基于确定的目标隐私数据所对应的管控规则对目标隐私数据的使用合规性进行管控，从而通过目标隐私数据所对应的管控规则对目标隐私数据的使用过程进行管控，进而能够对用户隐私数据的生产、流转、拷贝、销毁等处理过程进行管控，以实现对用户隐私数据的保护。

实施例五

[78]进一步地，基于上述图1至图3所示的方法，本说明书一个或多个实施例还提供了一种存储介质，用于存储计算机可执行指令信息，一种具体的实施例中，该存储介质可以为U盘、光盘、硬盘等，该存储介质存储的计算机可执行指令信息在被处理器执行时，能实现以下流程：获取目标隐私数据的处理请求；确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息；基于所述目标隐私数据对应的隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建；在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

[79]本说明书实施例中，还包括：将所述目标隐私数据加入到需要预设的隐私保护切面进行管控的队列中；所述获取目标隐私数据的处理请求，包括：当检测到所述目标隐私数据的处理接口接收到所述目标隐私数据的处理请求时，获取所述目标隐私数据的处理请求。

[80]本说明书实施例中，所述隐私保护切面包括隐私保护第一子切面和隐私保护第二子切面，所述隐私保护第一子切面用于在当前终端设备中对所述目标隐私数据的处理进行管控，所述隐私保护第二子切面用于对从当前终端设备输出所述目标隐私数据的处理进行管控，所述将所述目标隐私数据加入到需要预设的隐私保护切面进行管控的队列中，包括：基于所述目标隐私数据的处理请求，将所述目标隐私数据加入到需要所述隐私保护第一子切面和/或所述隐私保护第二子切面进行管控的队列中；所述在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控，包括：在对所述处理请求进行响应的过程中，当通过所述隐私保护第一子切面检测到所述目标隐私数据被采集和/或被消费时，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控；和/或，在对所述处理请求进行响应的过程中，当通过所述隐私保护第二子切面检测到所述目标隐私数据被流转和/或被拷贝时，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

[81]本说明书实施例中，所述处理请求包括所述目标隐私数据的流转请求、所述目标隐私数据的拷贝请求、所述目标隐私数据的采集请求、所述目标隐私数据的销毁请求和所述目标隐私数据的消费请求中的一种或多种。

[82]本说明书实施例中，所述隐私数据属性信息包括所述目标隐私数据的数据类型和/

或归属方信息，所述数据类型包括位置类、环境类和生物识别类。

[83]本说明书实施例中，所述目标隐私数据所对应的管控规则包括所述目标隐私数据的生命周期的管控子规则、流转行为的管控子规则和权限管控子规则中的一种或多种。

[84]本说明书实施例中，所述生命周期的管控子规则由所述目标隐私数据的有效时长、流转次数和拷贝次数中的一项或多项维度的信息构建。

[85]本说明书实施例中，所述流转行为的管控子规则由所述目标隐私数据的流转目标、流转方式和流转方向中的一项或多项维度的信息构建。

[86]本说明书实施例中，还包括：获取所述目标隐私数据的相关信息，所述目标隐私数据的相关信息包括所述目标隐私数据对应的隐私数据属性信息、所述目标隐私数据的生命周期信息、所述目标隐私数据的流转行为信息和所述目标隐私数据的权限相关信息中的一种或多种；基于所述目标隐私数据的相关信息，确定所述目标隐私数据所对应的管控规则。

[87]本说明书实施例提供一种存储介质，通过拦截目标隐私数据的处理请求，确定目标隐私数据对应的隐私数据属性信息，该隐私数据属性信息包括对目标隐私数据的使用进行管控所需的一个或多个维度的信息，然后，基于目标隐私数据对应的隐私数据属性信息，确定目标隐私数据所对应的管控规则，目标隐私数据所对应的管控规则为基于专家知识库构建，进而在该处理请求进行响应的过程中，基于确定的目标隐私数据所对应的管控规则对目标隐私数据的使用合规性进行管控，从而通过目标隐私数据所对应的管控规则对目标隐私数据的使用过程进行管控，进而能够对用户隐私数据的生产、流转、拷贝、销毁等处理过程进行管控，以实现用户对用户隐私数据的保护。

[88]上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[89]在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进(例如，对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件(Programmable Logic Device, PLD)(例如现场可编程门阵列(Field Programmable Gate Array, FPGA))就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言(Hardware Description Language, HDL)，而 HDL 也并非仅有一种，而是有许多种，如 ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDH(Ruby Hardware Description Language)等，目前最普遍使用的是 VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[90] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit, ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[91] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[92] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书一个或多个实施例时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[93] 本领域内的技术人员应明白，本说明书的实施例可提供为方法、系统、或计算机程序产品。因此，本说明书一个或多个实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[94] 本说明书的实施例是参照根据本说明书实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程欺诈案例的串并设备的处理器以产生一个机器，使得通过计算机或其他可编程欺诈案例的串并设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[95] 这些计算机程序指令也可存储在能引导计算机或其他可编程欺诈案例的串并设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[96] 这些计算机程序指令也可装载到计算机或其他可编程欺诈案例的串并设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[97] 在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

[98] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

[99] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

[100] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[101] 本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书一个或多个实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[102] 本说明书一个或多个实施例可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书一个或多个实施例，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[103] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[104] 以上所述仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书的权利要求范围之内。

权利要求书

1、一种基于隐私保护的数据风险防控方法，所述方法包括：

获取目标隐私数据的处理请求；

确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息；

基于所述目标隐私数据对应的隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建；

在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

2、根据权利要求1所述的方法，所述方法还包括：

将所述目标隐私数据加入到需要预设的隐私保护切面进行管控的队列中；

所述获取目标隐私数据的处理请求，包括：

当检测到所述目标隐私数据的处理接口接收到所述目标隐私数据的处理请求时，获取所述目标隐私数据的处理请求。

3、根据权利要求2所述的方法，所述隐私保护切面包括隐私保护第一子切面和隐私保护第二子切面，所述隐私保护第一子切面用于在当前终端设备中对所述目标隐私数据的处理进行管控，所述隐私保护第二子切面用于对从当前终端设备输出所述目标隐私数据的处理进行管控，

所述将所述目标隐私数据加入到需要预设的隐私保护切面进行管控的队列中，包括：

基于所述目标隐私数据的处理请求，将所述目标隐私数据加入到需要所述隐私保护第一子切面和/或所述隐私保护第二子切面进行管控的队列中；

所述在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控，包括：

在对所述处理请求进行响应的过程中，当通过所述隐私保护第一子切面检测到所述目标隐私数据被采集和/或被消费时，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控；

和/或，

在对所述处理请求进行响应的过程中，当通过所述隐私保护第二子切面检测到所述目标隐私数据被流转和/或被拷贝时，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

4、根据权利要求3所述的方法，所述处理请求包括所述目标隐私数据的流转请求、所述目标隐私数据的拷贝请求、所述目标隐私数据的采集请求、所述目标隐私数据的销毁请求和所述目标隐私数据的消费请求中的一种或多种。

5、根据权利要求1所述的方法，所述隐私数据属性信息包括所述目标隐私数据的数据类型和/或归属方信息，所述数据类型包括位置类、环境类和生物识别类。

6、根据权利要求1所述的方法，所述目标隐私数据所对应的管控规则包括所述目标隐私数据的生命周期的管控子规则、流转行为的管控子规则和权限管控子规则中的一种或多种。

7、根据权利要求6所述的方法，所述生命周期的管控子规则由所述目标隐私数据

的有效时长、流转次数和拷贝次数中的一项或多项维度的信息构建。

8、根据权利要求 6 所述的方法，所述流转行为的管控子规则由所述目标隐私数据的流转目标、流转方式和流转方向中的一项或多项维度的信息构建。

9、根据权利要求 1 所述的方法，所述方法还包括：

获取所述目标隐私数据的相关信息，所述目标隐私数据的相关信息包括所述目标隐私数据对应的隐私数据属性信息、所述目标隐私数据的生命周期信息、所述目标隐私数据的流转行为信息和所述目标隐私数据的权限相关信息中的一种或多种；

基于所述目标隐私数据的相关信息，确定所述目标隐私数据所对应的管控规则。

10、一种基于隐私保护的数据风险防控装置，所述装置包括：

请求获取模块，获取目标隐私数据的处理请求；

属性获取模块，确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息；

管控规则确定模块，基于所述目标隐私数据对应的隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建；

管控模块，在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

11、根据权利要求 10 所述的装置，所述装置还包括：

队列设置模块，将所述目标隐私数据加入到需要预设的隐私保护切面进行管控的队列中；

所述请求获取模块，当检测到所述目标隐私数据的处理接口接收到所述目标隐私数据的处理请求时，获取所述目标隐私数据的处理请求。

12、根据权利要求 11 所述的装置，所述隐私保护切面包括隐私保护第一子切面和隐私保护第二子切面，所述隐私保护第一子切面用于在当前终端设备中对所述目标隐私数据的处理进行管控，所述隐私保护第二子切面用于对从当前终端设备输出所述目标隐私数据的处理进行管控，

所述队列设置模块，基于所述目标隐私数据的处理请求，将所述目标隐私数据加入到需要所述隐私保护第一子切面和/或所述隐私保护第二子切面进行管控的队列中；

所述管控模块，在对所述处理请求进行响应的过程中，当通过所述隐私保护第一子切面检测到所述目标隐私数据被采集和/或被消费时，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控；和/或，在对所述处理请求进行响应的过程中，当通过所述隐私保护第二子切面检测到所述目标隐私数据被流转和/或被拷贝时，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

13、根据权利要求 10 所述的装置，所述目标隐私数据所对应的管控规则包括所述目标隐私数据的生命周期的管控子规则、流转行为的管控子规则和权限管控子规则中的一种或多种。

14、一种基于隐私保护的数据风险防控设备，所述基于隐私保护的数据风险防控设备包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器：

获取目标隐私数据的处理请求；

确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息；

基于所述目标隐私数据对应的隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建；

在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。

15、一种存储介质，所述存储介质用于存储计算机可执行指令，所述可执行指令在被执行时实现以下流程：

获取目标隐私数据的处理请求；

确定所述目标隐私数据对应的隐私数据属性信息，所述隐私数据属性信息包括对所述目标隐私数据的使用进行管控所需的一个或多个维度的信息；

基于所述目标隐私数据对应的隐私数据属性信息，确定所述目标隐私数据所对应的管控规则，所述目标隐私数据所对应的管控规则为基于专家知识库构建；

在对所述处理请求进行响应的过程中，基于确定的所述目标隐私数据所对应的管控规则对所述目标隐私数据的使用合规性进行管控。