



**Экономический  
и Социальный Совет**

Distr.: General  
31 January 2007  
Russian  
Original: English

**Комиссия по предупреждению преступности  
и уголовному правосудию**

Шестнадцатая сессия

Вена, 23-27 апреля 2007 года

Пункт 4 предварительной повестки дня\*

**Мировые тенденции в области преступности и меры  
борьбы с ней: объединение и координация усилий  
Управления Организации Объединенных Наций  
по наркотикам и преступности и государств-членов  
в области предупреждения преступности и уголовного  
правосудия**

**Результаты второго совещания Межправительственной  
группы экспертов по подготовке исследования  
о мошенничестве и преступном неправомерном  
использовании и фальсификации личных данных**

Доклад Генерального секретаря

Добавление

**Преступления, связанные с использованием личных данных**

Содержание

	<i>Пункты</i>	<i>Стр.</i>
I. Введение .....	1-5	3
А. Характер преступлений, связанных с использованием личных данных . .	1-2	3
В. Использование терминологии в настоящем исследовании .....	3-5	4
II. Основа системы удостоверения личности: средства идентификации, используемые государствами-членами .....	6-8	6

\* E/CN.15/2007/1.



	A. Публичные и частные системы идентификации .....	6	6
	B. Концепция идентификационной информации .....	7-8	6
III.	Преступления, связанные с использованием личных данных .....	9-12	8
	A. Имевшие место виды преступлений .....	9	8
	B. Средства совершения преступлений, связанных с использованием личных данных .....	10-11	9
	C. Ответные правовые меры .....	12	10
IV.	Взаимосвязь между преступлениями, связанными с использованием личных данных, и другими факторами .....	13-26	11
	A. Преступления, связанные с использованием личных данных, и экономическое мошенничество .....	13-14	11
	B. Другие преступления, связанные с преступлениями, совершаемыми с использованием личных данных .....	15-17	13
	C. Преступления, связанные с использованием личных данных, и организованная преступность .....	18	15
	D. Преступления, связанные с использованием личных данных, и терроризм .....	19-21	15
	E. Преступления, связанные с использованием личных данных, и отмыwanie денежных средств .....	22	17
	F. Преступления, связанные с использованием личных данных, и коррупция .....	23	18
	G. Преступления, связанные с использованием личных данных, и информационные, коммуникационные и коммерческие технологии ...	24	18
	H. Транснациональные элементы и необходимость международного сотрудничества в борьбе с преступлениями, связанными с использованием личных данных .....	25-26	19
V.	Уровень и тенденции преступности, связанной с использованием личных данных .....	27	20
VI.	Издержки преступности, связанной с использованием личных данных .....	28-29	21
VII.	Предупреждение преступлений, связанных с использованием личных данных .....	30	22

## I. Введение

### A. Характер преступлений, связанных с использованием личных данных

1. Возможность однозначно устанавливать личность конкретного лица<sup>1</sup> имеет чрезвычайно важное значение практически для любого аспекта социальной, политической и экономической деятельности. Для идентификации конкретного субъекта необходимо создать личные данные и увязать их с этим субъектом. Созданная идентификационная информация должна предусматривать возможность ее передачи, хранения и извлечения, и обычно ее увязывают с другой информацией, идентифицирующей конкретное лицо, такой как национальная принадлежность или гражданство, данные учета финансовой и банковской деятельности, сведения о прошлой судимости и прочая информация персонального и коммерческого характера. Поскольку личные данные играют основополагающую роль в самых разнообразных системах, они могут находить чрезвычайно широкое применение в преступной деятельности, если имеется возможность для изменения или фальсификации исходных идентификационных данных или для нарушения нормального функционирования систем создания, изменения, извлечения и проверки личных данных и другой информации. Поэтому вопросы, касающиеся личных данных, в той или иной мере рассматриваются в системах уголовного права и уголовного правосудия почти всех государств.

2. На настоящем этапе законодательная и директивная деятельность большинства государств ограничивается решением проблемы личных данных главным образом в контексте преступлений, которые могут быть совершены в дальнейшем в результате неправомерного использования личных данных. Тем не менее в последнее время некоторые государства начали рассматривать эту проблему в плоскости проблематики собственно личных данных. Предлагается наряду с криминализацией неправомерного использования личных данных выделить в новый и самостоятельный состав уголовного преступления основные, подготовительные или вспомогательные действия, такие как завладение личными данными, их копирование или подделывание и различные формы нарушения нормальной работы систем учета личных данных. Это согласуется с другими событиями последнего времени, включая принятие Конвенции Организации Объединенных Наций против транснациональной организованной преступности (резолюция 55/25 Генеральной Ассамблеи, приложение I) и Конвенции о киберпреступности Совета Европы<sup>2</sup>.

---

<sup>1</sup> Государствам было предложено описание мошеннического использования личных данных, которое включало действия, связанные с использованием личных или идентификационных данных как юридических, так и физических лиц, но им не задавались конкретные вопросы относительно идентификации юридических лиц. В своих ответах ряд государств отметили корпоративные регистры или аналогичные системы, используемые для идентификации юридических лиц, однако для оценки конкретных проблем, связанных с идентификацией юридических лиц, было получено недостаточно информации.

<sup>2</sup> См., например, статью 5 Конвенции об организованной преступности, касающуюся криминализации участия в организованной преступной группе, и статью 8 Конвенции о киберпреступности (Council of Europe, *Treaty Series*, No. 185), которая содержит требование криминализации связанных с компьютерами действий, преследующих цель совершения

Криминализация преступлений, основанных на использовании личных данных, свидетельствует о признании того факта, что исходные неправомерные действия в отношении личных данных могут привести к совершению различных последующих преступлений, что позволяет системе уголовного правосудия вмешиваться на более ранней стадии. Этот подход отражает также то обстоятельство, что, если для совершения других преступлений используются подлинные личные данные, ущерб наносится как лицу, которое идентифицируется такими подлинными личными данными, так и объектам совершаемых преступлений, которых следует рассматривать в качестве жертв преступления. Криминализация преступлений, связанных с использованием личных данных, отражает также признание того факта, что идентификационные данные и документы, удостоверяющие личность, особенно в случаях участия организованных преступных групп, приобретает характер незаконного товара, который передается правонарушителями, совершившими преступления, связанные с использованием личных данных, другим лицам, совершающим последующие преступления с использованием этой информации или изготовленных на ее основе поддельных удостоверений личности.

## **В. Использование терминологии в настоящем исследовании**

3. В своей резолюции 2004/26 Экономический и Социальный Совет просил Генерального секретаря созвать совещание Консультативной группы с целью подготовки исследования "О мошенничестве и преступном неправомерном использовании и фальсификации личных данных" и связанных с ним преступлениях. Как видно из обзорного вопросника, использовавшегося для сбора информации, на начальных этапах своей работы эксперты не рассматривали конкретное значение этих терминов и не пытались провести разграничение между мошенническим использованием личных данных и хищением личных данных. Лишь одно государство представило определение, взятое из его законодательства, в то время как большинство государств лишь указали, что предложенное в вопроснике определение (E/CN.15/2005/CRP.5, вопрос 33) в полной мере отражает проблемы, с которыми они сталкиваются. Эксперты постановили на предварительной основе и без ущерба для последующей деятельности использовать термин "мошенническое использование личных данных", но при рассмотрении полученных от государств ответов и других материалов стало очевидным, что некоторые упоминаемые неправомерные действия были аналогичны хищению, другие в большей степени напоминали мошенничество, а третьи содержали отдельные элементы обоих видов преступлений или не содержали их вовсе и точнее всего могут быть охарактеризованы как "смежные преступления".

4. Для обозначения всех форм противоправных действий, связанных с использованием личных данных, включая хищение личных данных и мошенническое использование личных данных, используется общий термин "преступления в отношении личных данных". Применение такого рассчитанного на перспективу подхода вызвано необходимостью, поскольку большинство

---

мошенничества, независимо от того, было ли оно закончено. Положения, в целом предусматривающие необходимость принятия мер в отношении основных, подготовительных и вспомогательных деяний, содержатся в обеих конвенциях.

государств еще не приняло законодательства в отношении таких преступлений. В целом преступления в отношении личных данных включают подготовительные противоправные действия или действия, образующие состав преступления, такие как подделка и выдача себя за другое лицо. Одна из трудностей выработки определения заключается в том, что злоупотребление личными данными может затрагивать сами идентификационные данные или другую связанную с ними информацию. Последний случай нельзя квалифицировать как преступление в отношении личных данных, хотя обычно такое преступление будет иметь те же последствия. Чтобы охватить такие ситуации, для целей настоящего исследования используется более общий термин "преступления, связанные с использованием личных данных". В некоторых контекстах используется также термин "злоупотребление личными данными". Он имеет аналогичное значение, но не содержит подразумеваемого предположения о том, что данное деяние уже квалифицируется как уголовное преступление или что его следует криминализировать. Концепция использования ложных личных данных или фальсификации личных данных или документов, удостоверяющих личность, включает три вида противоправных действий: составление или фабрикация полностью вымышленных личных данных; изменение подлинных личных данных или использование части подлинных личных данных; и использование подлинных личных данных лицом, иным, чем лицо, которому действительно принадлежат эти данные, или, если это касается документов, которое является законным владельцем документа<sup>3</sup>.

5. Термином "хищение личных данных" обычно обозначаются случаи, когда информация, относящаяся к личным данным, которая может включать базовую идентификационную информацию и, в некоторых случаях, другие персональные данные, фактически изымается таким образом, который аналогичен краже или мошенничеству, включая хищение материальных документов и нематериальной информации, которые были оставлены без внимания или находятся в свободном доступе, и принуждение путем обмана к добровольной выдаче документов или информации. Термином "мошенническое использование личных данных" обычно обозначается использование документов, удостоверяющих личность, или личных данных с целью совершения других преступлений или чтобы избежать обнаружения и уголовного преследования каким-либо образом. Что касается этого термина, то заложенный в нем элемент обмана заключается не в использовании обмана с целью получения информации, а в последующем использовании информации с целью обмана других лиц. Как и в контексте экономического мошенничества, элемент обмана включает введение в заблуждение как людей, так и технических систем.

---

<sup>3</sup> *Подготовительные материалы, касающиеся переговоров о разработке Конвенции Организации Объединенных Наций против транснациональной организованной преступности и протоколов к ней* (издание Организации Объединенных Наций, в продаже под № R.06.V.5), часть вторая, ст. 12, раздел С, примечание для толкования (b), и часть третья, ст. 12, раздел С, примечание для толкования (b).

## **II. Основа системы удостоверения личности: средства идентификации, используемые государствами-членами**

### **A. Публичные и частные системы идентификации**

6. Большинство государств сообщили о наличии инфраструктуры идентификации как в публичном, так и в частном секторе, и большинство из них сообщили о применении различных методов идентификации в зависимости от конкретной сферы применения. Что касается идентификации в публичном секторе, то некоторые государства сообщили о наличии централизованных национальных систем идентификации, однако большинство государств прибегают в основном к средствам идентификации конкретного назначения, таким как водительские права, паспорта, свидетельства о рождении, свидетельства о гражданстве и документы, удостоверяющие личность, которые используются в системе государственного налогообложения или социального обеспечения. В частном секторе средства идентификации, как правило, выдаются для конкретных коммерческих целей, например, для осуществления банковских операций или для целей кредитования, хотя компании, специализирующиеся в этой области, предпринимали шаги по использованию более общих форм идентификации. В некоторых странах применяются оба подхода, а в ряде государств федеративного устройства на уровне отдельных штатов или провинций действуют самостоятельные системы учета личных данных, что обуславливает необходимость разработки общих стандартов для проверки на национальном и международном уровнях. В случае отсутствия общенациональной системы конкретные формы идентификации, как правило, используются в целях, выходящих за рамки их назначения, что вызвано как необходимостью, так и – в случае применения принципа избыточности – задачей обеспечения дополнительной надежности. Согласно имеющейся информации, самой распространенной формой коммерческой идентификации в частном секторе является кредитная карточка. Мнения относительно общенациональных систем идентификации различаются. В некоторых странах общенациональные требования идентификации получили широкое признание. В других странах выдвигаемые предложения вызывают значительные разногласия и встречают возражения, объясняемые опасностью ущемления гражданских свобод. Одно из государств отметило, что его национальная система идентификации все шире используется в коммерческих целях, и поставило вопрос о том, не следует ли предложить коммерческим структурам взять на себя часть высоких расходов по эксплуатации централизованной системы.

### **B. Концепция идентификационной информации**

7. Большинство государств впервые столкнулось с концепцией идентификационной информации. Нормативно-правовое признание она получила лишь в некоторых государствах, хотя государства, изучающие проблему преступности, связанной с использованием личных данных, начали обращать на нее внимание. Вместо этого большинство государств упоминало документы, удостоверяющие личность, или персональную информацию. Персональная информация включает идентификационную информацию, а также

другую информацию персонального или личного характера о статусе или деятельности идентифицируемых лиц, которая не всегда бывает достаточной для идентификации физического лица. Многие государства сообщили о разработке положений уголовного законодательства и других мер для защиты персональной информации, включая всю идентификационную информацию или значительную ее часть. Многие государства сообщили также о таких преступлениях, как хищение, подделка, незаконная торговля или незаконное хранение или использование, которые совершаются в отношении конкретных видов документов, удостоверяющих личность, таких как паспорт. Один из важных аспектов концепции идентификационной информации состоит в том, что образующие ее элементы, необходимые для установления личности, обычно оказываются недостаточными для этой цели, если берутся по отдельности. Наиболее широко распространенные документы, удостоверяющие личность, обычно содержат целый ряд элементов идентификационной информации, а автоматизированные средства идентификации, такие как дебетовые и кредитные карточки, как правило, предусматривают наличие по крайней мере двух элементов, один из которых относится к карточке или документу, а другой – к лицу, которое они идентифицируют. Вопрос о том, из чего складываются личные данные, в определенной степени может зависеть от особенностей культуры и местных традиций. Согласно обычаям некоторых стран, имя, которое дается человеку, включает имена его родителей, название места происхождения семьи, а также название профессии или рода занятий. Другой фактор связан с тем, в какой мере традиционное личное опознавание постепенно заменялось сначала бумажными документами, удостоверяющими личность, а в последнее время, по мере появления новых форм идентификационной информации, вытесняется электронной идентификацией.

8. Согласно полученной информации, в бумажные документы чаще всего включают различные имена, в том числе имя и фамилию данного человека, имена его родителей, дату и место рождения и текущее место жительства или коммерческого предприятия. Информация электронных систем включает полное имя или сокращенное имя пользователя, пароль, персональный идентификационный номер (PIN), аутентификационный номер для осуществления банковских операций (TAN), цифровые подписи и другие криптографические приложения. Новую область разработки вспомогательных технических средств образуют различные биометрические идентификаторы, включая характеристики ДНК, отпечатки пальцев, фотографии, "голосовые отпечатки", изображения радужной оболочки и сетчатки глаза. В силу простоты использования наиболее широкое распространение получили фотографии. Применение других биометрических идентификаторов обеспечивает высокую степень надежности, но требует больших расходов и вызывает обеспокоенность в отношении соблюдения конфиденциальности, вследствие чего они широко используются лишь в таких областях, как составление досье на преступников, где высокие расходы оправдываются необходимостью обеспечения надежности и другими факторами. О наличии соответствующего законодательства и других положений сообщили два государства. Одно из них использовало термин "идентификационные данные" для обозначения электронной информации, обеспечивающей идентификацию в рамках автоматизированных систем. Другое государство представило определение термина "средства идентификации", используемого для обозначения элемента преступления, связанного с хищением

личных данных. В его законодательстве "средства идентификации" определяются как "любое имя или число, которые могут использоваться по отдельности или в сочетании с любой другой информацией для идентификации конкретного лица".

### **III. Преступления, связанные с использованием личных данных**

#### **A. Имевшие место виды преступлений**

9. Государства сообщили о целой серии преступлений, связанных с неправомерным использованием или фальсификацией личных данных. Наиболее широко распространены такие преступления, как подделка документов, удостоверяющих личность, и различные виды действий, связанных с выдачей себя за другое лицо. Наряду с преступлениями в отношении документов, удостоверяющих личность, отмечались преступления, которые были направлены на системы или процессы создания, установления или проверки личных данных. Одна из форм нарушения функционирования систем учета личных данных заключается, в частности, в попытке путем обмана или подкупа добиться выдачи действительного документа, удостоверяющего личность, лицу, которое не имеет на него право. О преступлениях такого характера сообщили несколько государств, отметивших, в том числе, обычные преступления, связанные с дачей взяток и коррупцией, и более конкретные преступления, связанные с использованием ложной или вводящей в заблуждение информации с целью получения лицензий или других документов, удостоверяющих личность. Некоторые формы незаконного получения идентификационной информации охватываются действующим законодательством о хищениях, но оно может применяться не во всех случаях. Поскольку нематериальная информация не может рассматриваться как имущество, правовые нормы, касающиеся хищений, не могут применяться в тех случаях, когда информация берется из таких источников, как списанные документы. В отношении таких действий, как "фишинг", может применяться действующее законодательство об экономическом мошенничестве, если можно установить, что идентификационные данные, добытые путем обмана, имеют ценность. Отдельные государства сообщили о наличии правовых норм, касающихся других преступлений, включая незаконное хранение, передачу или незаконный сбыт идентификационных данных или такой информации, как компьютерные пароли и данные кредитных карточек. Ряд государств выразили обеспокоенность в связи с тем, что преступники могут извлекать большой объем идентификационной информации путем взлома компьютерных программ. Ряд государств отмечали преступления, связанные с выдачей себя за другое лицо, в том числе путем использования личных данных другого лица, подделки и использования личных данных несуществующего лица.



## **В. Средства совершения преступлений, связанных с использованием личных данных**

10. Полученные ответы на вопросник свидетельствуют о том, что средства совершения преступлений, связанных с использованием личных данных, в некоторой степени зависят от характера и назначения соответствующих структур идентификации и средств, имеющихся в распоряжении правонарушителей. В большинстве случаев совершения таких преступлений идентификационная информация изымается, копируется или умело фабрикуется, воплощается в некую удобную для пользования форму и затем используется. Правонарушители получают идентификационную информацию путем хищения или копирования целых документов либо путем завладения различными способами частью информации для создания личных данных и получения подлинных документов. Некоторые государства сообщили о случаях получения личных данных на лицо, умершее в молодом возрасте, и их использования для подачи поддельного заявления на выдачу свидетельства о рождении и других базовых документов, удостоверяющих личность, с целью постепенно создать целостный образ конкретного человека. Многие государства выражали обеспокоенность в связи с преступлениями, основанными на использовании личных данных, жертвами которых становятся лица, пользующиеся информационными технологиями. Наиболее широкое распространение получил метод под названием "фишинг" или "фарминг", при котором пользователей компьютерных сетей путем обмана принуждают сообщать правонарушителям имя пользователя, пароль и другую электронную идентификационную информацию. Через электронную почту или веб-сайты жертвы получали сообщения, поступавшие якобы от поставщиков услуг или других ведомств, в которых запрашивалась идентификационная информация. Веб-сайты нередко размещались в странах, удаленных как от правонарушителей, так и от жертв, и одно из государств сообщило, что путем отслеживания ему удалось обнаружить такие веб-сайты по крайней мере в десяти разных странах. Имели место и другие формы киберпреступности, включая распространение вредоносных программ, заражающих отдельные компьютеры, извлекающих персональную информацию и передающих ее правонарушителю, и взлом коммерческих веб-сайтов с целью получения данных кредитных карточек и другой идентификационной информации о клиентах. Идентификационная информация, особенно в больших объемах, превратилась в незаконный товар, сбываемый другим правонарушителям. Коммерческие структуры, беспокоящиеся о конфиденциальности своих клиентов, уже становились жертвами вымогательства, когда правонарушители завладевали информацией и угрожали предать ее гласности в случае невыплаты денег.

11. Ряд государств сообщили о методах, используемых с целью получения идентификационной информации по дебетовым и кредитным карточкам в основном с целью последующего использования в рамках экономического мошенничества. Часть информации получают путем проведения карточки через специальное считывающее устройство. Что касается дебетовых карточек, то такие устройства устанавливаются на банкоматах (АТМ) вместе с миниатюрными видеокамерами для отслеживания клиентских кодов. Другие государства сообщали о случаях получения идентификационной информации должностными лицами, имеющими доступ к правительственным или

коммерческим системам, либо правонарушителями, не имеющими доступа к таким системам, но получающими такую информацию с помощью взяток и других методов коррупции. Полученная идентификационная информация зачастую может использоваться сразу же с целью выдачи себя за жертву, в то время как для использования материальных документов, удостоверяющих личность, как правило, требуется принятие некоторых дополнительных мер. Материальные документы, удостоверяющие личность, становятся все более совершенными, и для их подделки требуются дополнительные специальные знания, ресурсы и оборудование. Поэтому факт наличия таких документов позволяет предположить участие или поддержку со стороны организованных преступных групп. В то же время современные информационно-коммуникационные технологии породили некоторые средства подделки, легко доступные для многих отдельных правонарушителей, что послужило толчком к развитию как средств обеспечения защиты документов, так и методов преступной деятельности. Преступления, связанные с использованием личных данных, совершаются не только путем подделки материальных документов, но и путем нарушения работы систем, с которыми связаны такие документы.

### **С. Ответные правовые меры**

12. В том, что некоторые формы злоупотребления личными данными следует выделить в состав уголовного преступления и они должны подлежать наказанию, в целом наблюдается единодушие, но при этом высказываются разные мнения в отношении того, какие именно виды деяний следует криминализировать. Большинство государств включили преступления, связанные с использованием личных данных, в более общие составы преступлений. При этом только шесть государств сообщили, что они криминализировали полностью или частично передачу, хранение и использование идентификационных или личных данных другого лица или вымышленных личных данных в связи с совершением другого преступления, и лишь одно из них, Соединенные Штаты Америки, предусмотрело уголовную ответственность за хищение личных данных как таковое. В соответствующих нормативных актах Соединенных Штатов содержится определение "средств идентификации" и предусмотрена уголовная ответственность за умышленное хранение, передачу и использование такой информации без соответствующих законных полномочий. Ряд других государств указали, что они изучают основное содержание преступлений, основанных непосредственно на злоупотреблении личными данными, включая завладение идентификационной информацией, ее фабрикации и неправомерное использование, в том числе использование с целью совершения других уголовных преступлений. Почти все государства указали, что они предусмотрели уголовную ответственность по крайней мере за некоторые конкретные виды действий, охватываемые определением мошеннического использования личных средств, которое предложено в вопроснике, или связанные с ними действия. Чаще всего сообщалось о таких преступлениях, как подделка и выдача себя за другое лицо. Кроме того, в более общие составы преступления, такие как подделка, был включен ряд конкретных форм злоупотребления личными данными, в том числе подделка документов, удостоверяющих личность, и преступления, связанные с использованием компьютеров, такие как хищение данных и

несанкционированный доступ к компьютерным системам или нарушение их нормального функционирования. Некоторые государства сообщили о криминализации противоправных действий в отношении документов, удостоверяющих личность, или личных данных, которые считаются особенно важными, таких как паспорта или правительственные удостоверения личности. Согласно статье 7 Конвенции о киберпреступности, государствам – участникам этой конвенции надлежит принять все меры к тому, чтобы их нормативные акты о подделке охватывали подделку, связанную с использованием компьютеров или электронных данных. Ряд государств сообщили о преступлениях, связанных с компьютерным "фишингом" и аналогичными действиями. В других государствах такая деятельность также может охватываться более общими правовыми нормами о киберпреступности, включающими, в частности, вопросы хищения или незаконного хранения паролей.

#### **IV. Взаимосвязь между преступлениями, связанными с использованием личных данных, и другими факторами**

##### **A. Преступления, связанные с использованием личных данных, и экономическое мошенничество**

13. В настоящем исследовании проводится разграничение между экономическим мошенничеством и преступлениями, связанными с использованием личных данных, но как показывает опыт, на практике эти две области смыкаются друг с другом. Такого же мнения придерживаются некоторые правительства, поскольку их специалисты в области экономического мошенничества выполняют значительную часть работы в новой области борьбы с преступностью, связанной с использованием личных данных. Это одна из причин, побудивших Комиссию по предупреждению преступности и уголовному правосудию к проведению настоящего исследования на совместной основе. Как уже отмечалось, злоупотребление личными данными в сфере экономического мошенничества выполняет практически ту же роль, что и в других видах преступлений, при том что во многих мошеннических комбинациях злоупотреблению личными данными принадлежит дополнительная роль в плане введения жертв в заблуждение. Это подтверждается многочисленными примерами. Лица, занимающиеся экономическим мошенничеством, выдают себя за публичных должностных лиц с целью извлечения информации или с целью получения в результате мошеннической операции поступлений от предыдущей мошеннической сделки на основании поддельного требования. Во многих сообщениях об экономическом мошенничестве и мошенничестве с использованием средств связи часто отмечался факт выдачи себя за должностных лиц банков, учреждений, выдающих кредитные карточки, и поставщиков услуг связи. Кроме того, поддельные удостоверения личности часто использовались с целью совершения хищений личных данных, особенно "фишинга", в ходе которого правонарушители используют удостоверения личности соответствующих ведомств с целью получения от жертв путем обмана компьютерных паролей и других видов идентификационной информации. Некоторые государства сообщили о действиях, которые могут образовывать основу такого состава преступления, как хищение личных данных и

мошенническое использование личных данных, являющегося частью более общего состава мошеннических операций. Мошеннические действия, такие как мошенническое использование кредитных карточек, также могут рассматриваться как мошенническое использование личных данных, поскольку преступник использует дублированную или похищенную карточку в качестве средства идентификации, выдавая тем самым себя за законного владельца карточки. В коммерческих системах, таких как система распространения кредитных карточек, базовые элементы личных данных зачастую настолько тесно связаны с коммерческим аспектом, что на практике оказывается весьма сложно или даже невозможно провести разграничение между мошенническим использованием личных данных и экономическим мошенничеством.

14. Главное различие между мошенничеством и преступлениями, связанными с использованием личных данных, заключалось в том, что согласно юридическим определениям и правовым нормам почти всех государств, представивших информацию, мошенничество квалифицируется как экономическое преступление. Соответственно, необходимо доказать наличие определенного материального ущерба, нанесенного жертве, или выгоды, извлеченной преступниками. В действительности же преступления, связанные с использованием личных данных, не всегда являются экономическими по своему характеру и могут совершаться в качестве содействия другим преступлениям, которые могут и не быть экономическими по своему характеру. Это различие может найти отражение в применении Конвенции об организованной преступности. Конвенция применяется лишь в тех случаях, когда имеет место деятельность организованной преступной группы, и квалифицирует такую группу организованной преступной группой, если одна из ее целей состоит в том, чтобы получить "финансовую или иную материальную выгоду"<sup>4</sup>. Таким образом, организованная группа, преследующая исключительно неэкономические цели, например террористическая группа, и любые совершаемые ею преступления в отношении личных данных не будут входить в сферу применения Конвенции. Тем не менее, помимо терроризма, она будет охватывать подавляющее большинство случаев. Во-первых, в Конвенции четко разъясняется, что с получением финансовой или иной материальной выгоды должны быть связаны цели группы, а не какие-либо конкретные преступления, которые она может совершить или в которых она может участвовать. Это означает, что неэкономические преступления, связанные с использованием личных данных, входят в сферу применения Конвенции, если они связаны с деятельностью организованной преступной группы, которая занимается также экономической преступностью. Конвенция будет применяться в тех случаях, когда преступления в отношении личных данных совершаются для содействия торговле людьми, незаконному ввозу мигрантов, отмыванию денежных средств или другим формам незаконного ввоза или торговли, даже если на начальных стадиях расследования не было обнаружено никакой очевидной связи, кроме участия в деятельности самой группы. Во-вторых, термин "финансовая или иная материальная выгода" является сравнительно широким и включает, в частности, торговлю материалами детской порнографии с целью получения услуг

---

<sup>4</sup> См. Конвенцию об организованной преступности, статья 2, подпункт (а), и статья 3, пункт 1.

сексуального характера (A/55/383/Add.1, пункт 3)<sup>5</sup>. Он охватывает преступления в отношении личных данных, при которых похищенные или сфабрикованные удостоверения личности или идентификационная информация рассматриваются в качестве незаконного товара, являющегося объектом купли, продажи или обмена, а также случаи неправомерного использования средств идентификации для получения личной или коллективной выгоды, в том числе нефинансового характера, такой как возможность въезда в другую страну. В-третьих, судя по полученной информации, преступления, связанные с использованием личных данных, чаще всего сопряжены с экономическими преступлениями, такие как мошенничество, и преступлениями, связанными с использованием документов на въезд/выезд и удостоверений личности, которые входят в сферу применения Протокола о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, и Протокола против незаконного ввоза мигрантов по суше, морю и воздуху, которые дополняют Конвенцию Организации Объединенных Наций против организованной преступности (резолюция 55/25 Генеральной Ассамблеи, приложения II и III). Предполагается, что они преследуют цель получения финансовой или иной материальной выгоды, за исключением случаев, когда мигранты незаконно ввозятся по гуманитарным соображениям или в других не противоречащих закону целях<sup>6</sup>.

## **В. Другие преступления, связанные с преступлениями, совершаемыми с использованием личных данных**

15. Указанные в сообщениях виды связи между преступлениями, связанными с использованием личных данных, и другими преступлениями можно разделить на три группы в зависимости от того, каким образом используются вымышленные или чужие личные данные: во-первых, для получения доступа к помещениям или электронным счетам с целью совершения других преступлений; во-вторых, для сокрытия подлинных личных данных преступника, с тем чтобы избежать обнаружения, возникновения помех и уголовного правосудия; и, в-третьих, в случае экономического мошенничества, как главный элемент введения в заблуждение в рамках мошеннической операции.

16. Хотя связь между злоупотреблением личными данными и другими преступлениями, как правило, касается личных данных правонарушителя, может возникать и проблема злоупотребления личными данными жертвы. Во многих страновых сообщениях о торговле людьми отмечается, что преступники изымали паспорта жертв или другие принадлежавшие им документы, удостоверяющие личность, и использовали их как средство осуществления

---

<sup>5</sup> *Подготовительные материалы...*, часть первая, статья 2, раздел С, примечание для толкования (d). См. также A/AC.254/4/Rev.1, сноска 4, A/AC.254/4/Rev.2, сноска 16, и A/AC.254/4/Rev.7, сноска 22.

<sup>6</sup> Определение "незаконный ввоз мигрантов" должно включать ссылку на положение о "финансовой или иной материальной выгоде", с тем чтобы государствам-участникам не требовалось устанавливать уголовную ответственность за незаконный ввоз мигрантов в целях, не противоречащих закону, в частности, по гуманитарным соображениям или на основе тесных семейных связей (см. Протокол о мигрантах, статья 2, подпункт (a), и *Подготовительные материалы...*, часть третья, статья 3, раздел С, примечание для толкования (a)).

контроля над ними или предупреждения их бегства. Хотя в Протоколе о торговле людьми не предусмотрено требование криминализации действий, связанных с изъятием удостоверений личности, как одного из элементов торговли людьми, некоторые государства-участники приняли такие меры<sup>7</sup>. В пункте 1 статьи 7 Конвенции Организации Объединенных Наций о правах ребенка (резолюция 44/25 Генеральной Ассамблеи, приложение) закреплено право на регистрацию сразу же после рождения как средство установления личности, а при рассмотрении дел о геноциде и этнической чистке отмечалась проблема систематического изъятия удостоверений личности<sup>8</sup>.

17. Преступления, связанные с использованием личных данных, как правило, сопряжены с экономическим мошенничеством и другими аналогичными преступлениями отчасти вследствие того, что экономическое мошенничество чрезвычайно широко распространено в большинстве государств и злоупотребление личными данными имеют ключевое значение для успешного осуществления большинства мошеннических операций. Ряд государств отметили, что преступления в отношении личных данных совершаются в контексте деятельности по отмыванию денежных средств с целью обмануть системы выявления доходов от преступной деятельности и подозрительных операций. Многие государства выражали особое беспокойство в связи с преступлениями в отношении личных данных, касающимися паспортов и других удостоверений личности, предназначенных для осуществления поездок, считая, что они представляют проблему как в плане преступности, так и в плане безопасности, поскольку паспортная система является важным средством предотвращения въезда на территорию страны известных террористов, уголовных преступников и незаконных мигрантов. Неправомерные действия в отношении паспортов также были связаны с организованной преступностью, в частности с торговлей людьми и незаконным ввозом мигрантов, и ряд государств, обративших внимание на связь между этими явлениями, сообщили о значительных масштабах незаконного ввоза мигрантов или торговли людьми, что объяснялось географическим положением соответствующих стран. Ряд государств сообщили о разработке новых паспортов, включающих дополнительные меры защиты. Был выявлен ряд факторов, объединяющих киберпреступность и преступность, связанную с использованием личных данных. Наряду с получением от жертв путем обмана компьютерной идентификационной информации ряд государств отметили факты использования поддельных удостоверений личности и кредитных карточек для получения неподдающихся отслеживанию услуг в области связи с целью совершения других преступлений, в том числе террористических актов.

<sup>7</sup> См., например, *Уголовный кодекс Канады*, раздел 279.03 об изъятии или уничтожении документов на въезд/выезд и документов, удостоверяющих личность, Свод законов Канады 2005 года, глава 43.

<sup>8</sup> См., например, *Prosecutor of the International Criminal Tribunal for the former Yugoslavia v. Slobodan Milosevic et al*, Case No. IT-99-37-PT, Second Amended Indictment (29 October 2001), paragraph 61 (<http://www.un.org/icty/indictment/english/mil-2ai011029e.htm>).

### **C. Преступления, связанные с использованием личных данных, и организованная преступность**

18. Ряд государств сообщили о взаимосвязи между преступлениями, связанными с использованием личных данных, и деятельностью организованных преступных групп. Чаще всего она проявлялась в случаях организованного экономического мошенничества, отмывания денежных средств, организованной торговли людьми и незаконного ввоза мигрантов, а также использования мошеннических операций с целью получения неподдающихся отслеживанию услуг в области связи. Все эти вопросы рассматриваются в других разделах настоящего доклада. Помимо совершения преступлений, связанных с использованием личных данных, в рамках другой преступной деятельности, такой как отмывание денежных средств, некоторые организованные преступные группы, достигшие достаточно высокого уровня развития, могут заниматься преступной деятельностью, заключающейся непосредственно в использовании личных данных. Судя по ответам государств, выделяются два основных направления такой деятельности. Организованные преступные группы могут совершать преступления, связанные с использованием личных данных, с целью защиты своих членов и своей деятельности от мер по надзору за незаконными операциями, а также для осуществления регулярных непротивозаконных мероприятий, таких как международные поездки. Некоторые факты свидетельствуют также о специализации групп и использовании документов, удостоверяющих личность, и идентификационной информации в качестве незаконного товара. Такие группы могут накопить достаточные знания для изготовления все более совершенных документов, удостоверяющих личность, или использовать слабые места в системе выдачи документов и путем обмана или подкупа властей получать подлинные документы, которые затем могут продаваться другим лицам для использования при совершении преступлений, террористических актов, незаконных поездок, незаконного въезда в другие страны или другой деятельности, осуществление которой с помощью законных документов, удостоверяющих личность, было бы небезопасным. Некоторые организованные преступные группы настолько хорошо подготовлены и оснащены, что они могут использовать многоступенчатые методы изменения личных данных, с помощью которых идентификационная информация из одного источника используется для подачи поддельных заявлений на выдачу подлинных документов с целью создания и обеспечения еще более надежных и выверенных вымышленных личных данных.

### **D. Преступления, связанные с использованием личных данных, и терроризм**

19. Вопрос о взаимосвязи между преступлениями, связанными с использованием личных данных, и терроризмом затронули лишь некоторые государства. В этом вопросе их главная причина для беспокойства по сути была той же, что и в связи с организованной преступностью и другими проблемами: террористические организации могут совершать преступления, связанные с использованием личных данных, с целью получения идентификационной информации и документов, удостоверяющих личность, которые, в свою очередь, могут быть использованы террористами с целью избежать надзора или ареста,

который скорее всего был бы неизбежен, если бы они действовали в своем подлинном качестве. Больше всего внимания государства уделяли удостоверениям личности, предназначенным для поездок, и международным перемещениям лиц, подозреваемых в террористической деятельности<sup>9</sup>, но те же вопросы возникали в контексте идентификации и деятельности исключительно на национальном уровне, поскольку террористам приходится избегать привлечения к себе внимания и в повседневной деятельности, такой как вождение автомобиля или осуществление банковских операций, и поскольку обычные внутренние средства удостоверения личности представляют собой основу для получения более надежных средств удостоверения личности, таких как паспорт, и трудоустройства, а также других соответствующих документов, удостоверяющих личность, которые требуются для доступа к более надежно защищаемым объектам, таким как аэропорты.

20. Информация, полученная экспертами из других официальных источников, содержит примеры того, как лица, подозреваемые в террористической деятельности, получали и использовали документы, удостоверяющие личность, с целью избежать наблюдения и пристальной проверки. Для этого использовались поддельные или измененные документы и подлинные документы, полученные на чужое имя, основные данные которых, такие как имя, фамилия и дата рождения, не позволяют установить подлинную личность владельца документа или выявить его преступное прошлое. Отмечался также такой метод, как использование поддельных или содержащих ложную информацию заявлений на выдачу новых документов. Лица, сочувствующие террористическим организациям, могут просто выдать требующиеся им документы, и затем сделать ложное заявление об утрате или хищении этих документов, а подозреваемые, чьи паспорта отражают подозрительный характер поездок, могут уничтожить их и ложным путем получить вместо них другие документы<sup>10</sup>. Как и в контексте экономического мошенничества, некоторые государства высказывали также в данном контексте обеспокоенность в связи с использованием базовых мошеннических операций в отношении поставщиков телекоммуникационных услуг с целью получения на анонимной основе не поддающихся отслеживанию услуг в области мобильной телефонной связи, сети Интернет или других средств связи.

21. В случае отсутствия четких доказательств связанное с терроризмом преступление, включающее использование личных данных, порой очень сложно отличить от других смежных преступлений, особенно организованных преступлений. Многие базовые схемы деятельности широко применяются как организованными преступными группами, так и террористическими группами, и террористические группы, которые не располагают достаточным собственным опытом и знаниями, могут просто закупать поддельные документы, удостоверяющие личность, у организованных преступных групп. Преступления, связанные с использованием личных данных, могут совершаться с целью финансирования терроризма так же, как и с целью отмывания денежных средств.

<sup>9</sup> См., например, доклад Генерального секретаря, озаглавленный "Единство в борьбе с терроризмом: рекомендации по глобальной контртеррористической стратегии (A/60/825, пункт 62).

<sup>10</sup> См., например, *Report of the National Commission on Terrorist Attacks upon the United States*, chapter 5.3, pp.168-169 (<http://www.9-11commission.gov/report/index.htm>).



## Е. Преступления, связанные с использованием личных данных, и отмывание денежных средств

22. Многие меры противодействия отмыванию денежных средств в значительной степени зависят от наличия информации о личности преступников или отдельных идентификационных данных, и преступления, связанные с использованием личных данных, относятся к числу средств, используемых преступниками с целью отмывания доходов. Одним из основных элементов механизма противодействия отмыванию денежных средств, помимо системы финансового учета и уведомления о подозрительных сделках, является возможность устанавливать личность клиентов и сторон финансовых сделок, иногда обозначаемая как принцип "знай своего клиента"<sup>11</sup>. Выявление сторон сделки позволяет установить, что средства или активы являются доходами от совершенных преступлений, или помочь в проведении расследования исходных или основных правонарушений. На более поздних этапах имеющиеся идентификационные данные о всех сторонах, участвовавших в серии переводных операций по отмыванию денежных средств, как правило, имеют чрезвычайно важное значение для уголовного преследования правонарушителей, осуществления следственных мероприятий по отслеживанию доходов и других полученных в результате средств или активов, а также установления взаимозависимости или связи между основными правонарушениями и конечной формой и местонахождением доходов с такой степенью определенности, которая позволяет произвести конфискацию в судебном порядке. Надежная система установления личности служит также средством сдерживания или предупреждения основных преступлений<sup>12</sup>. Некоторые государства отмечали, что различные методы отмывания денежных средств включают использование информационных, коммуникационных и коммерческих технологий, позволяющих генерировать фиктивные идентификационные данные и производить дистанционный перевод средств на основании этих фиктивных идентификационных данных, а также обеспечивающих условия для осуществления большого объема законных переводов средств, среди которых могут быть сокрыты отмываемые активы. Эти технологии вызвали также колоссальное расширение масштабов практики международных переводов и офшорных банковских операций, что создает дополнительные трудности для регулирующих ведомств и открывает перед значительно более широким кругом правонарушителей возможности осуществления офшорных банковских операций и сокрытия средств. В то же время новые технологии способствовали соответствующему развитию вспомогательных средств, применяемых в сфере предупреждения преступности, обеспечения безопасности и осуществления следственной деятельности.

<sup>11</sup> См., например, *Конвенцию об организованной преступности*, статья 7, пункт 1 (а); *Конвенцию Организации Объединенных Наций против коррупции*, статья 14; и рекомендацию 5 из 40 рекомендаций Целевой группы по финансовым мероприятиям для борьбы с отмыванием денег ([http://www.fatf-gafi.org/document/28/0,2340,en\\_32250379\\_32236930\\_33658140\\_1\\_1\\_1\\_1,00.html#40recs](http://www.fatf-gafi.org/document/28/0,2340,en_32250379_32236930_33658140_1_1_1_1,00.html#40recs)).

<sup>12</sup> См. P. A. Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (World Bank, 2003), chap. VI, part A.

## **F. Преступления, связанные с использованием личных данных, и коррупция**

23. Государствам-членам не предлагалось рассматривать вопрос о том, как соотносятся между собой преступления, связанные с использованием личных данных, и коррупция, однако эксперты высказали свое мнение по некоторым возможным связывающим их аспектам. Как и при совершении других правонарушений, преступления, связанные с использованием личных данных, могут использоваться в качестве средства, позволяющего избежать обнаружения или уголовной ответственности при совершении коррупционных действий. Например, поддельные удостоверения личности могут использоваться с целью запутать расследование таких преступлений, как хищение. Как и при совершении преступлений, связанных с отмыванием денежных средств, злоупотребление личными данными может преследовать цель предотвратить отслеживание и конфискацию доходов от коррупции. Другой важный аспект этой взаимосвязи заключается в использовании коррупции в качестве вспомогательного средства совершения преступлений, связанных с использованием личных данных. Например, поскольку становится весьма сложным подделывать паспорта и другие аналогичные документы, зачастую значительно проще воспользоваться методом активного и пассивного подкупа должностных лиц с целью получения подлинного документа. Аналогичным образом коррупционные действия могут совершаться с целью изменения или фальсификации данных в системах проверки или подтверждения личных данных. По мнению экспертов, это направление является сравнительно новым, и они считают, что такие ситуации, по-видимому, будут возникать в будущем по мере накопления преступниками соответствующего опыта.

## **G. Преступления, связанные с использованием личных данных, и информационные, коммуникационные и коммерческие технологии**

24. Как и в сфере экономического мошенничества, информационные и коммуникационные технологии могут играть разную роль в преступлениях, связанных с использованием личных данных. В некоторых рассмотренных случаях такие технологии играли ключевую роль в процессе совершения преступлений, связанных с использованием личных данных, а в других случаях они представляли собой лишь один из элементов более общего состава преступления. Более широкое использование технических средств в процессах идентификации вместо личного контакта открывает перед преступниками новые возможности, позволяющие выдавать себя за другое лицо, поскольку, кем бы ни был на самом деле правонарушитель, для того чтобы обмануть автоматизированную систему, достаточно знать пароли и другие соответствующие идентификаторы. Кроме того, технологии, получающие все более широкое распространение, открывают перед многими сравнительно слабо разбирающимися в технических вопросах преступниками возможности использования сложных средств подделки как материальных, так и электронных документов. Новые технологии позволяют также внедряться в системы выдачи документов и получать подлинные документы. В то же время технические

достижения содержат элементы, способствующие предупреждению или пресечению преступлений, связанных с использованием личных данных. Некоторые из этих элементов являются неотъемлемой частью новых технологий, другие специально включаются в них как средство предупреждения преступлений или упрощения процесса обнаружения и расследования, третьи разрабатываются и предлагаются специально для борьбы с новыми видами преступлений по мере появления или совершенствования последних. К числу средств защиты относятся материальные элементы, затрудняющие изготовление документов, например фотографии, микропечать, голограммы и компьютерные микросхемы, для производства которых все же требуется сравнительно сложное оборудование и специальные знания. Кроме того, современные надежные средства связи позволяют быстро проверять документы, удостоверяющие личность, по нескольким надежным базам данных, а информационные технологии делают этот процесс настолько оперативным, что он может с успехом применяться на практике в таких областях, как проверка паспортов на контрольно-пропускных пунктах. Одно из государств отметило, что, по возможности, оно все шире применяет процедуру "многофакторной" идентификации, предусматривающей использование нескольких самостоятельных идентификаторов разных категорий, по которым производится перекрестный контроль, когда необходимо установить или проверить личность. К ним относятся элементы трех основных категорий: элементы, которыми физически владеет данное лицо, такие как дебетовая или кредитная карточка, национальное удостоверение личности или паспорт; элементы, известные только данному лицу, такие как пароли и персональные идентификационные номера; и биометрические элементы (биологические параметры, принадлежащие только данному лицу).

## **Н. Транснациональные элементы и необходимость международного сотрудничества в борьбе с преступлениями, связанными с использованием личных данных**

25. Ряд государств сообщили, что они сталкивались со случаями совершения преступлений, связанных с использованием личных данных, транснационального характера. Большинство из них касались преступлений, связанных с паспортами и другими удостоверениями личности, предназначенными для поездок. К ним относятся преступления, связанные непосредственно с документами, удостоверяющими личность, такие как подделка, изменение, неправомерное использование подлинных документов и неправомерные действия в отношении процессов выдачи документов, а также другие преступления, совершаемые в том числе посредством неправомерного использования этих удостоверений личности, такие как торговля людьми, незаконный ввоз мигрантов и другие преступления, связанные с незаконным ввозом или незаконной миграцией. Идентификационная информация в цифровой форме без труда передается между странами. Другую наиболее часто упоминаемую категорию преступлений, связанных с использованием личных данных и обладающих транснациональными аспектами, образует киберпреступность.

26. Ряд государств обратили особое внимание на важность международного сотрудничества в расследовании транснациональных преступлений, связанных с использованием личных данных, и осуществление соответствующего уголовного преследования, однако о конкретных формах требуемого сотрудничества в этой области сообщалось не много. Как и в случае с экономическим мошенничеством, большинство государств считают достаточным использование таких существующих структур, как Конвенция об организованной преступности, Конвенция Организации Объединенных Наций против коррупции и Конвенция о киберпреступности. Ряд государств особо отметили также практическую пользу использования Интерпола, Европейского полицейского управления (Европол) и аналогичных организаций в качестве механизмов сотрудничества. По мнению большинства государств, в этой области требуются такие же формы сотрудничества, как и в области борьбы с транснациональным мошенничеством и другими формами киберпреступности. Большинство основных преступлений, совершаемых с помощью похищенных и сфабрикованных личных данных, скорее всего будут рассматриваться как "серьезные преступления", как они определены в подпункте (b) статьи 2 Конвенции против организованной преступности, но поскольку государства намерены рассматривать злоупотребление личными данными в качестве отдельного состава преступления, неизбежно возникнет вопрос о том, входят ли в сферу применения Конвенции такие новые особые преступления. Ряд государств отметили, что как и в борьбе с киберпреступностью, оперативность оказания официальной помощи и неофициального сотрудничества порой имеет решающее значение. В этой связи при расследовании дел о мошенничестве, требующих электронных доказательств, особенно когда требуется безотлагательная помощь, было бы целесообразно иметь круглосуточно работающую сеть. Один из вопросов, затронутый лишь некоторыми государствами, был связан с тем, что помимо материальных убытков преступления, связанные с использованием личных данных, причиняют ущерб личности подлинных физических и юридических лиц, чьи личные данные были объектом неправомерного использования. Репутации и доброму имени может быть нанесен значительный ущерб, а меры по их восстановлению не входят в сферу осуществления сотрудничества по уголовным вопросам большинства государств.

## **V. Уровень и тенденции преступности, связанной с использованием личных данных**

27. Большинство государств, представивших данные или оценки, высказали мнение о расширении масштабов преступности, связанной с использованием личных данных, а ряд государств отметили, что она расширяется чрезвычайно стремительными темпами. Наблюдаемое расширение масштабов такой преступности связано не только с повышением общего уровня преступности и количества совершаемых преступлений, но также с диверсификацией видов преступлений. Лишь два государства заявили о сокращении масштабов преступности, связанной с использованием личных данных, а ряд государств указали, что они не располагают достаточной информацией или что имеющаяся информация не позволяет прийти к какому-то определенному выводу. Большинство государств смогли представить лишь заключения или оценки экспертов, и лишь одно государство представило статистическую информацию.

Оно представило такую информацию за продолжительный период, что позволило сделать заключение о том, что хищение личных данных представляет собой значительную и растущую проблему. Сама концепция была настолько новой, что всякое резкое увеличение показателей могло объясняться отчасти повышением уровня осведомленности общественности об этой проблеме, повышением к ней внимания со стороны правительства и сравнительно недавним созданием механизмов представления информации, однако имевшиеся данные совершенно ясно свидетельствовали о значительном увеличении количества таких случаев. Сообщалось также о значительных экономических потерях, но было неясно, в какой мере эти потери были вызваны экономическим мошенничеством или другими вторичными преступлениями, совершенными путем хищения личных данных, и в какой мере эти потери были вызваны другими причинами, такими как нанесение ущерба репутации жертв и издержки, связанные с восстановлением доброго имени. Одно из государств сообщило об исследовании, проведенном с целью определить количество веб-сайтов в сети Интернет, использовавшихся с целью "фишинга", в результате чего было установлено, что за период 2005-2006 годов количество таких веб-сайтов возросло втрое. Если эти цифры являются точными, то они, возможно, отражают следующую картину: масштабы новых форм преступности резко вырастают за короткий период по мере распространения информации о методах осуществления таких преступлений, а затем выравниваются вследствие повышения уровня осведомленности общественности и принятия соответствующих контрмер. Некоторые из государств, указавших на расширение масштабов преступности, связанной с использованием личных данных, отметили ряд возможных причин такого расширения, включая коррупцию среди должностных лиц и в сфере коммерческой деятельности, возможности, появившиеся в результате все более широкого использования компьютерных технологий, и трудности разработки и применения на практике технических мер, позволяющих проверять личные данные и в целом не отставать от темпов развития методов преступной деятельности. Отсутствие четких национальных определений мошеннического использования личных данных и других аналогичных преступлений исключает возможность соответствующего статистического анализа и позволяет проводить лишь самые общие сопоставления между странами или регионами.

## **VI. Издержки преступности, связанной с использованием личных данных**

28. Ни одно из государств, приславших ответы, не представило подробной информации о фактических издержках преступности, связанной с использованием личных данных, и лишь некоторые из них дали оценку общего объема потерь. Ряд государств указали, что в условиях отсутствия конкретных правовых норм, касающихся таких правонарушений, нельзя даже помышлять о сборе и анализе точной статистической информации. Некоторые государства отметили, что с учетом характера хищения личных данных представляется весьма сложным провести границу между издержками и убытками от преступлений в отношении личных данных как таковых и издержками других преступлений, таких как мошенничество, совершенных с использованием поддельных личных данных или чужих личных данных. Государства, которые

представили общую калькуляцию потерь, обобщили все потери, понесенные в результате всех основных правонарушений, связанных с преступлениями в отношении личных данных, и такой же подход был использован некоторыми коммерческими структурами. С учетом некоторых представленных примеров было признано чрезвычайно сложным оценить в денежном выражении некоторые виды нанесенного вреда и ущерба, такого как потеря репутации, или – учитывая непрерывность процесса нанесения ущерба – определить соответствующую продолжительность для его измерения.

29. В то же время одно из государств отметило, что можно сделать качественную оценку. Согласно его предложению, вред и ущерб включают: экономические и неэкономические потери, которые могут понести лица, чьи личные данные были неправомерно использованы; расходы, время и усилия, потребовавшиеся для ликвидации ущерба репутации и доброму имени; экономические и неэкономические потери от других преступлений, совершенных с использованием фиктивных личных данных; государственные и коммерческие издержки, связанные с мероприятиями в области предупреждения, расследования и уголовного преследования; общее снижение эффективности в результате принятия мер по обеспечению безопасности; и издержки, связанные с утратой или снижением уровня доверия потребителей к коммерческим операциям. Помимо вопросов осуществления базовой количественной оценки возникают также принципиальные вопросы о том, как следует распределять некоторые из этих издержек между публичными и коммерческими структурами и как следует распределять полученные в качестве компенсации средства, когда имеются различные жертвы или интересы, пострадавшие в результате преступлений, связанных с использованием личных данных.

## **VII. Предупреждение преступлений, связанных с использованием личных данных**

30. Некоторые государства сообщили о таких мерах предосторожности и контроля, как ограничение срока действия документов, требование их обновления, технические решения, затрудняющие внесение в документы изменений, и осуществление проверки действительности документа, удостоверяющего личность, в каждом случае его использования. Некоторые государства отметили необходимость создания технических систем и подготовки должностных лиц для повышения эффективности таких проверок и выявления поддельных документов. Представленная государствами информация свидетельствует о возможности применения целого ряда конкретных методов для предупреждения преступлений, связанных с использованием личных данных. Меры обеспечения надежности документов включают как меры, призванные затруднить подделку документов, так и системные меры, призванные защитить подлинные документы и системы выдачи документов от хищений, утечки и выдачи в результате коррупции<sup>13</sup>. Могут быть приняты меры по совершенствованию практики установления действительности и проверки документов, особенно путем использования систем связи и баз данных,

---

<sup>13</sup> См. подпункты (a) и (b) статьи 12 Протокола о торговле людьми и Протокола о мигрантах.

защищенных криптографическими средствами и аналогичными мерами, которые используются для сопоставления документа и его держателя со справочной информацией в момент использования этого документа. Для увязки личных данных с конкретными физическими характеристиками могут использоваться биометрические показатели. В целом могут проводиться контрольные мероприятия для оценки общей надежности системы, охватывающие все ее элементы, включая: выдачу и аннулирование документов; обновление документов и информации; методы обеспечения защиты информации; срок действия и цикл обновления документов; и общее взаимодействие систем и мер обеспечения защиты.

---