Организация Объединенных Наций E/CN.15/2013/25

Экономический и Социальный Совет

Distr.: General
19 February 2013
Russian
Original: English

Комиссия по предупреждению преступности и уголовному правосудию
Двадцать вторая сессия
Вена, 22-26 апреля 2013 года
Пункт 7 предварительной повестки дня*
Мировые тенденции в области преступности и новые проблемы в области предупреждения преступности и уголовного правосудия и способы их решения

Вербальная нота Постоянного представительства Аргентинской Республики при Организации Объединенных Наций (Вена) от 19 февраля 2013 года, адресованная Управлению Организации Объединенных Наций по наркотикам и преступности

Постоянное представительство Аргентинской Республики при Организации Объединенных Наций (Вена) свидетельствует свое уважение Управлению Организации Объединенных Наций по наркотикам и преступности и имеет честь препроводить согласно резолюции 2011/35 Экономического и Социального Совета от 28 июля 2011 года доклад шестого совещания группы ведущих экспертов по преступлениям с использованием личных данных, которое было проведено в Вене 16-18 января 2013 года, с просьбой распространить его в качестве официального документа двадцать второй сессии Комиссии по предупреждению преступности и уголовному правосудию, которая состоится в Вене 22-26 апреля 2013 года.

Постоянное представительство Аргентинской Республики при Организации Объединенных Наций (Вена) пользуется этой возможностью для того, чтобы вновь выразить Управлению Организации Объединенных Наций по наркотикам и преступности заверения в своем высочайшем уважении.

* E/CN.15/2013/1.

V.13-80751 (R) 250213 260213

Приложение к вербальной ноте Постоянного представительства Аргентинской Республики при Организации Объединенных Наций (Вена) от 19 февраля 2013 года, адресованной Управлению Организации Объединенных Наций по наркотикам и преступности

Доклад о работе шестого совещания группы ведущих экспертов по преступлениям с использованием личных данных

Вена, 16-18 января 2013 года*

I. Введение

1. После выхода в 2007 году исследования Организации Объединенных Наций о "мошенничестве и преступном неправомерном использовании и фальсификации личных данных", которое было проведено по поручению ЮНОДК и представлено Комиссии по предупреждению преступности и уголовному правосудию на ее шестнадцатой сессии[1], и на основе своих мандатов, предусмотренных резолюциями 2004/26 и 2007/20 ЭКОСОС, ЮНОДК учредило консультационную платформу по проблеме преступлений с использованием личных данных. Цель этой платформы заключалась в том, чтобы способствовать проведению встреч правительственных экспертов, представителей частного сектора, а также научных экспертов и представителей международных и межправительственных организаций с целью обобщения опыта, разработки стратегий, содействия проведению дальнейших исследований и согласования практических мер по противодействию преступлениям с использованием личных данных. Эта платформа начала действовать благодаря работе группы ведущих экспертов, которая была учреждена в 2007 году.

2. На своих предыдущих пяти совещаниях группа ведущих экспертов представила ряд руководящих принципов и направлений будущей деятельности, которые включают, помимо прочего, проведение дальнейших исследований; расширенные консультации с частным сектором; подготовку научно-исследовательских работ; составление подборок материалов с примерами соответствующего законодательства; разработку материалов по оптимальным путям и средствам содействия международному сотрудничеству в борьбе с преступлениями с использованием личных данных; и составление подборок материалов с примерами успешной практики в деле защиты потерпевших. Кроме того, работа группы ведущих экспертов привела к выпуску *Справочника по преступлениям с использованием личных данных* (2011 год), который содержит также практическое руководство по международному сотрудничеству в борьбе с преступлениями с использованием личных данных, предназначенное для использования в качестве справочного материала в программах технической помощи и деятельности по созданию

* Настоящий доклад официально не редактировался.

[1] E/CN.15/2007/8 и Add. 1-3.

потенциала с целью расширения экспертных знаний при решении правовых, институциональных и оперативных вопросов, связанных с преступлениями с использованием личных данных[2].

3. В своей резолюции 2011/35 от 28 июля 2011 года Экономический и Социальный Совет признал усилия Управления Организации Объединенных Наций по наркотикам и преступности по содействию работе группы ведущих экспертов по преступлениям с использованием личных данных.

4. В этой же резолюции Совет далее просил Управление Организации Объединенных Наций по наркотикам и преступности продолжать его усилия, в консультациях с Комиссией Организации Объединенных Наций по праву международной торговли, в целях содействия выработке общих пониманий и обмену мнениями между субъектами государственного и частного секторов по вопросам, связанным с экономическим мошенничеством и преступлениями с использованием личных данных, и, в частности, сфокусировать будущую работу группы ведущих экспертов по преступлениям с использованием личных данных на, в том числе, различных вопросах, связанных с привлечением ресурсов и экспертных знаний частного сектора к разработке мероприятий по оказанию технической помощи в этой области и их осуществлению.

5. В резолюции 2011/35 Совет просил также Управление Организации Объединенных Наций по наркотикам и преступности продолжать его усилия, через группу ведущих экспертов по преступлениям с использованием личных данных, по сбору информации и данных об угрозах, создаваемых экономическим мошенничеством и преступлениями с использованием личных данных в различных географических регионах.

6. Шестое совещание группы ведущих экспертов было проведено 16-18 января 2013 года в Вене в соответствии с мандатами, предусмотренными в резолюции 2011/35 ЭКОСОС.

II. Организация совещания

A. Открытие совещания

7. Совещание открыл 16 января 2013 года директор Отдела по вопросам международных договоров Управления Организации Объединенных Наций по наркотикам и преступности, который поблагодарил участников за их присутствие и упомянул о предшествующей работе группы ведущих экспертов. Он подчеркнул, что подход к составу этой группы предусматривает участие нескольких заинтересованными сторон для стимулирования обмена мнениями, информацией и опытом между различными сторонами, а также содействия их взаимопониманию и сотрудничеству в борьбе с преступлениями с использованием личных данных. Он также отметил, что группе ведущих экспертов удалось найти для вопроса о вызовах, создаваемых преступлениями с использованием личных данных как особой "новой и формирующейся"

[2] Более подробную информацию о работе группы ведущих экспертов, проделанной на ее предыдущих совещаниях, см. по адресу www.unodc.org/unodc/en/organized-crime/emerging-crimes.html#Identity_related_crime.

формой преступности, достойное место в повестке дня различных международных форумов в области предупреждения преступности и уголовного правосудия (Комиссия по предупреждению преступности и уголовному правосудию, Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, Конференция участников Конвенции Организации Объединенных Наций против транснациональной организованной преступности и Конференция государств – участников Конвенции Организации Объединенных Наций против коррупции).

8. В своих вступительных замечаниях Председатель группы ведущих экспертов посол Эухенио Куриа, представитель правительства Аргентины в Вене, напомнил о юридическом мандате, предусматривающем организацию совещания, и кратко представил каждую из тем, включенных в его повестку дня.

B. Участники

9. В совещании приняли участие следующие эксперты:

a) Публичный сектор

Эухенио Куриа, посол, Постоянный представитель Аргентины при Организации Объединенных Наций (Вена), Аргентина (Председатель группы ведущих экспертов); *Джон Ансуорт*, заместитель Директора – Начальник Отдела оперативной информации и мер, Национальное бюро оперативной информации о мошенничестве (НБИМ), полиция города Лондон, Соединенное Королевство; *Джонатан Раш*, заместитель Начальника по вопросам стратегии и политики, Секция борьбы с мошенничеством, Уголовный отдел, Министерство юстиции, Соединенные Штаты Америки;

b) Частный сектор

Анко Блокзейл, Председатель, "Сафран Морфо", Нидерланды; *Фонс Кнопейс*, Центр по работе с удостоверениями личности, Нидерланды; *Пэт Кейн*, постоянный научный сотрудник, Рабочая группа по борьбе с "фишингом" (APWG), Соединенные Штаты Америки; *Фердинанд Пьятти*, "Прайс Уотерхаус Куперс", Австрия; *Себастьян Сейар*, руководитель международных проектов, RESOCOM (Франция); *Мэтью Аллен*, Директор по вопросам финансовых преступлений, Британская ассоциация банкиров (БАБ), Соединенное Королевство; *Эндрю Вебстер*, старший менеджер по вопросам контроля за глобальными финансовыми преступлениями (EMEA), Британская ассоциация банкиров (БАБ), Соединенное Королевство; *Джонатан Шетфорд*, руководитель Отдела расследований (EMEA), Британская ассоциация банкиров (БАБ), Соединенное Королевство;

c) Международные и межправительственные организации

Чже Сун Ли, секретарь Рабочей группы IV – электронная торговля, Комиссия Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ); *Кейт Ланнан*, сотрудник по правовым вопросам, Отдел права международной торговли, Управление по правовым вопросам, Комиссия

Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ); *Кристофер Хорнек*, руководитель программы обеспечения безопасности проездных документов, Антитеррористическая группа (АТГ), Департамент по транснациональным угрозам (ДТНУ), Организация по безопасности и сотрудничеству в Европе (ОБСЕ); *Поль Пикар*, сотрудник по вопросам борьбы с терроризмом, Организация по безопасности и сотрудничеству в Европе (ОБСЕ);

d) Научные круги/отдельные эксперты

Жилберту Мартинш ди Алмейда, "Мартинш ди Алмейда Адвогадуш", Бразилия; *Марко Герке*, профессор уголовного права, Кельнский университет, Германия; *Никос Пассас*, Северо-Восточный университет, факультет криминологии и уголовного правосудия, Бостон, Соединенные Штаты Америки;

e) Секретариат

Димостенис Крисикос, сотрудник по вопросам предупреждения преступности и уголовного правосудия, ЮНОДК/ОМД/КСР/СКО; *Армо Шалтан*, младший сотрудник по вопросам предупреждения преступности и уголовного правосудия, ЮНОДК/ОМД/КСР/СКО; *Стивен Малби*, сотрудник по вопросам контроля над наркотиками и предупреждения преступности, ЮНОДК/ОМД/СОП/СКО.

C. Утверждение повестки дня

10. Участники совещания утвердили следующую повестку дня:

1. Открытие совещания
2. Утверждение повестки дня и организация работы
3. Преступления с использованием личных данных и киберпреступность
4. Сравнительные подходы: проблемы, вызываемые преступлениями с использованием личных данных в различных географических регионах
5. Основные элементы национальной стратегии в отношении преступлений с использованием личных данных: показательные примеры
6. Работа других международных и межправительственных организаций
7. Техническая помощь
   a) области для принятия мер: законодательные меры, управление использованием идентификационных данных и предупреждение преступлений с использованием личных данных

b) вовлечение частного сектора в разработку и осуществление программ технической помощи: партнерские отношения между публичным и частным секторами

8. Представление показательных примеров образовательных проектов, включающих элементы профилактики и выявления преступлений с использованием личных данных

9. Прочие вопросы

10. Выводы – рекомендации в отношении дальнейших действий.

III. Обсуждения

A. Преступления с использованием личных данных и киберпреступность

11. Секретариат проинформировал участников о прогрессе, достигнутом в отношении работы межправительственной группы экспертов по киберпреступности[3]. В этой связи было отмечено, что в своей резолюции 65/230 от 21 декабря 2010 года Генеральная Ассамблея одобрила Салвадорскую декларацию о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире, принятую двенадцатым Конгрессом Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. В этой резолюции Ассамблея просила Комиссию по предупреждению преступности и уголовному правосудию учредить, в соответствии с пунктом 42 Салвадорской декларации, межправительственную группу экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, включая обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве, с целью изучения возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых или иных мер по противодействию киберпреступности.

12. Первое совещание межправительственной группы экспертов по киберпреступности было проведено в Вене с 17 по 21 января 2011 года. На этом совещании группа экспертов рассмотрела и утвердила подборку тем и методологию для проведения исследования. Методология исследования предусматривала распространение вопросника среди государств-членов, межправительственных организаций и представителей частного сектора и научных учреждений. Ответы на вопросник были получены от 69 государств-членов из различных региональных групп. Кроме того, свои мнения высказали также 50 компаний. В соответствии с этой методологией сбор информации проводился Секретариатом с февраля 2012 года по июль 2012 года. Затем на основе собранной информации Секретариат подготовил резюме проекта исследования для его рассмотрения на втором совещании

[3] См. также E/CN.15/2013/24.

межправительственной группы экспертов по киберпреступности, которое было запланировано в Вене с 25 по 28 февраля 2013 года[4]. Решение о статусе исследования будет принято межправительственной группой экспертов.

13. Информация об уголовном законодательстве в области киберпреступности собиралась при помощи вопросника, подготовленного для целей проведения исследования, а также посредством анализа основных источников с использованием имеющейся информации о законодательстве более чем 100 стран. В вопроснике, подготовленном для целей проведения исследования, были выделены 14 деяний, которые обычно включаются в понятие киберпреступности. Страны-респонденты сообщили о практически повсеместной криминализации этих 14 деяний, за исключением в основном преступлений, связанных со спамом, и, в некоторой степени, преступлений, связанных со средствами неправомерного использования компьютеров, преступлений, связанных с расизмом и ксенофобией, а также использования Интернета с целью завлечения или "груминга" детей[5]. В том что касается указанных 14 деяний, то страны сообщили, что для совершения основных деяний, представляющих собой киберпреступления против конфиденциальности, неприкосновенности данных и доступности компьютерных систем, применяются специальные виды киберпреступности. В отношении других форм киберпреступности чаще использовались правонарушения общего характера (непосредственно не связанные с киберпреступностью). В то же время для совершения деяний, представляющих собой преступления с использованием личных данных, как сообщается, применяются оба метода. В случае последних правонарушений объектами зарегистрированных преступлений были различные цели, которые включали и личные данные, и идентификационную информацию.

14. Было отмечено, что в общемировых масштабах правоохранительные органы фиксируют рост уровня киберпреступности в связи с тем, что и частные лица, и организованные преступные группы используют новые возможности для совершения преступлений, руководствуясь стремлением к извлечению прибыли и получению личной выгоды. По оценкам, свыше 80 процентов киберпреступлений совершаются в той или иной форме организованной деятельности, со сложившимися черными рынками киберпреступности в области цикла создания вредоносных программ, компьютерных вирусов, управления бот-сетями, сбора персональных и финансовых данных, продажи данных и получения денег за финансовую информацию.

---

[4] См. UNODC/CCPCJ/EG.4/2013/2.

[5] Незаконный доступ к компьютерной системе; незаконный доступ, перехват или получение компьютерных данных; незаконное вмешательство в данные или вмешательство в систему; производство, распространение или хранение средств неправомерного использования компьютеров; нарушение конфиденциальности или мер защиты данных; компьютерное мошенничество или подлог; компьютерные преступления, связанные с использованием личных данных; компьютерные преступления, касающиеся авторских прав и товарных знаков; компьютерные преступления, связанные с причинением личного вреда; компьютерные преступления, связанные с расизмом или ксенофобией; использование компьютера с целью производства, распространения или хранения детской порнографии; использование компьютера для завлечения или "груминга" детей; и использование компьютера для содействия террористическим преступлениям.

15. Исследование также показало, что уровень виктимизации частных лиц в результате киберпреступности значительно выше, чем в случае "обычных" форм преступности. Показатели виктимизации в отношении мошенничества с кредитными картами в режиме онлайн, преступлений с использованием личных данных, ответов на попытку фишинга и несанкционированного доступа к учетным записям электронной почты составляют от 1 до 17 процентов среди пользователей Интернета в 21 стране мира, в то время как типичные показатели в отношении краж со взломом, ограблений и угонов автомобилей составляют для этих же стран не более 5 процентов. Показатели виктимизации, связанной с киберпреступностью, выше в странах с низким уровнем развития, что явно свидетельствует о необходимости принятия более активных превентивных мер в этих странах.

16. Группа ведущих экспертов подчеркнула необходимость активно заняться вопросом использования сложных схем совершения киберпреступлений, предусматривающих преступное неправомерное использование и фальсификацию личных данных. Один из участников отметил важность защиты потерпевших и информационно-просветительских программ в связи с увеличением числа случаев, когда граждане не принимают мер предосторожности для своей собственной надлежащей защиты. Некоторые участники указывали на необходимость наращивания потенциала в целях расширения национальных возможностей в деле борьбы с такими преступлениями, особенно в развивающихся странах.

B. Сравнительные подходы: проблемы, вызываемые преступлениями с использованием личных данных в различных географических регионах

17. В соответствии с практикой, сложившейся на ее предыдущих совещаниях, группа ведущих экспертов послужила платформой для сравнительного изложения вопросов, касающихся совершения преступлений с использованием личных данных в различных географических регионах. В этой связи были представлены два оратора: профессор Марко Герке рассказал о событиях, связанных с преступлениями с использованием личных данных, в Европейском союзе, бассейне Карибского моря и Азиатско-Тихоокеанском регионе, а г-н Жилберту Мартинш ди Алмейда представил новую правовую базу для борьбы с киберпреступностью и преступлениями с использованием личных данных в Бразилии.

18. Профессор Герке сначала отметил, что, хотя в рамках Европейского союза уголовное право по-прежнему в основном регулируется самими государствами, Лиссабонский договор по реформе впервые предоставил органам ЕС широкие полномочия, выходящие за рамки простого межправительственного сотрудничества в области уголовного права, включая киберпреступность. В настоящее время ведется работа над проектом директивы, направленной против детской порнографии, и проектом директивы по борьбе с атаками на информационные системы. Точно так же в статье 77 этого же договора предусмотрены полномочия, касающиеся "Политики в области пограничного контроля, предоставления убежища и иммиграции", куда входят и вопросы,

относящиеся к обеспечению достоверности и надежности документов, удостоверяющих личность.

19. План действий на 2010-2014 годы, принятый Европейским союзом в целях осуществления Стокгольмской программы об "Открытой и безопасной Европы на службе и защите граждан"[6], дает право рассматривать вопрос о представлении новых законодательных предложений, в том числе по борьбе с киберпреступностью и обеспечению безопасности информационных сетей. На этой основе в 2012 году началось осуществление "Исследования по оценке воздействия применительно к предложению относительно новой правовой базы для борьбы с хищениями идентификационных данных". Недавно Европейской комиссии был представлен проект исследования. В его содержании учитывалась работа группы ведущих экспертов, так как ЮНОДК просили обеспечить обратную связь на подготовительном этапе сбора информации. По мнению профессора Герке, неправомерное использование личных данных не может быть эффективно криминализировано в качестве особого состава без единой схемы управления идентификационными данными, а государства – члены Европейского союза пока еще не готовы к такому шагу.

20. Профессор Герке также представил три совместных проекта Европейского союза и Международного союза электросвязи (МСЭ), направленных на согласование законодательства в области киберпреступности в Карибском регионе, тихоокеанских островных странах и странах Африки к югу от Сахары путем разработки типовых законов и оказания технической помощи по вопросам осуществления в каждой стране. Первый проект в Карибском регионе, который в настоящее время близок к завершению, начался с полного обзора законодательства отобранных 15 стран, а также с проведения регионального сравнительного исследования с участием во всем этом процессе национальных экспертов. Была также разработана стратегия по внедрению нового законодательства в каждой стране. Проект в Карибском бассейне был направлен на повышение конкурентоспособности путем согласования политики, законодательства и нормативной базы в области ИКТ. Конструктивный подход привел к принятию выбранными странами стандартов в деле борьбы с киберпреступностью, которые выходят за рамки тех, что приняты в большинстве европейских стран. Устойчивый характер этого проекта был обеспечен путем привлечения национальных экспертов на протяжении всего процесса, начиная с самых ранних этапов, и организации для них специальной подготовки. Особо отмечалось, что одним из ключевых факторов успеха является та роль, которую страновые отделения играют в определении соответствующих субъектов. Информацию об уроках, извлеченных в ходе этого процесса, можно найти на веб-сайте МСЭ.

21. Такой же курс проводится и при осуществлении второго и третьего проектов, представленных профессором Герке. Второй проект был организован в 2011 году по просьбе тихоокеанских островных стран с целью обеспечить создание потенциала и подготовку кадров в том, что касается политики и нормативно-правового регулирования в сфере ИКТ. Третий проект в странах Африки к югу от Сахары направлен на согласование политики в области ИКТ в регионе, осуществление которого было начато в начале 2012 года.

---

[6] См. Official Journal of the European Union, C 115/1, 4 May 2010.

22. В ходе последовавшего затем обсуждения участники подчеркнули важность разработки таких стандартов, и в частности типовых законов, и особо отметили ту роль, которую Организация Объединенных Наций могла бы сыграть в этом отношении. Однако было также указано на то, что для стран, у которых уже есть такое законодательство, необходимо организовать процесс повышения информированности и учебные занятия по внедрению этих стандартов.

23. Г-н Жилберту Мартинш ди Алмейда рассказал об эволюции "законодательного ландшафта" в Бразилии в том, что касается киберпреступности. После краткого исторического экскурса он остановился на недавней "волне" нормативных мер, принятых в рамках комплексного подхода. Такое развитие событий было обусловлено проблемами, связанными с совершением преступлений с использованием личных данных, поскольку, как сообщается, каждые 15 секунд один потребитель в Бразилии становится жертвой такого преступления. Наиболее распространенными формами преступлений с использованием личных данных, с которыми пришлось столкнуться, являются хищение идентификационных данных путем охоты за кредитными картами; покупка электронных товаров и мобильных телефонов; и открытие банковских счетов при применении ложной или неправомерно используемой идентификационной информации. Было подчеркнуто, что в преступлениях, связанных с личными данными, произошел переход от использования вирусов к сканированию, то есть использованию автоматического поиска уязвимых мест. Было указано также, что атаки в основном носят внутринациональный характер.

24. Бразильская законодательная инициатива – это пакет, состоящий из 11 законопроектов, и часть из них уже одобрена (по борьбе с киберпреступностью и гражданским свободам). По остальным законодательным актам, включая закон о свободе информации, законы о киберпреступности, закон о защите личных данных, закон об электронных сделках, закон об электронной торговле (кодекс потребителя), закон о платежах, совершаемых с помощью мобильной связи, новые законы об Интернет-протоколах, процедурные (и технические) стандарты и нормативные правила (безопасность, SEC), успешно ведутся консультации с целью их окончательной доработки и утверждения.

25. В декабре 2012 года в один день были приняты два утвержденных законопроекта. Они дополняют друг друга, поскольку первый больше касается вопросов существа, а второй – вопросов процедурного характера. Взаимодополняемость этих двух законодательных актов означает проведение согласованного подхода. Об этом свидетельствует и использование в каждом из этих законов одной и той же терминологии, и тот факт, что они были разработаны с учетом одних и тех же международных стандартов (таких как стандарты ИСО), и их общая цель – предусмотреть как превентивные, так и карательные меры.

26. Г-н Мартинш ди Алмейда сообщил, что использованное в утвержденных законопроектах определение охватывает как проникновение, так и установку незащищенных элементов с целью получения незаконных преимуществ. Отягчающие обстоятельства предусмотрены для тех, кто производит, предлагает, распространяет, продает устройства или компьютерные программы

или расширяет сферу их действия с целью получения таких незаконных преимуществ, если получен доступ к содержанию частного электронного сообщения, коммерческой тайне или конфиденциальной информации, или установлен несанкционированный дистанционный контроль за устройством, или, в случае раскрытия, содержание полученной информации становится источником прибыли или передается третьим лицам как товар. Для различных национальных учреждений была создана единая платформа для установления стандартов и контроля за их соблюдением.

C. Основные элементы национальной стратегии в отношении преступлений с использованием личных данных: показательные примеры

27. В рамках этого пункта повестки дня доклады и обсуждения были посвящены главным образом разработке рамок для основных компонентов национальной стратегии в области предупреждения, расследования преступлений с использованием личных данных, уголовного преследования и наказания за их совершение. В этой связи Секретариат указал, что впервые вопрос о разработке национальной стратегии в отношении преступлений с использованием личных данных был поднят Экономическим и Социальным Советом в его резолюции 2009/22 (пункт 6 (f)). Секретариат также представил доклад, подготовленный докладчиком группы ведущих экспертов, который на совещании не присутствовал[7]. В этом документе приводится обзор вероятных заинтересованных сторон или участников национальной стратегии как из публичного, так и частного секторов. В нем также очерчен процесс, которого следует придерживаться при разработке, внедрении и осуществлении национальной стратегии. Кроме того, в документе изложены основные элементы национальной стратегии с уделением особого внимания начальному этапу оценки угроз и сбора и анализа соответствующей информации; установлению приоритетов и координации; законодательным элементам; компоненту, связанному с расследованием и обеспечением соблюдения закона; основополагающему фактору превентивной деятельности; созданию потенциала; вопросам, связанным с ресурсами; и механизмам расширения сотрудничества между публичным и частным секторами.

28. Национальная стратегия, принятая Соединенными Штатами Америки для решения проблем, вызываемых преступлениями с использованием личных данных, была представлена г-ном Джонатаном Рашем. Соединенные Штаты приняли в 1998 году Закон о противодействии хищению и присвоению идентификационных данных, в котором впервые был установлен состав хищения личных данных. На следующий год при Комитете министра юстиции по должностным преступлениям был создан Подкомитет по борьбе с хищениями идентификационных данных. В 2006 году была создана президентская Целевая группа по борьбе с хищениями идентификационных данных под председательством министра юстиции. В 2007 году Целевая группа приняла стратегический план.

[7] См. E/CN.15/2013/CRP.2.

29. Стратегия ориентирована на три этапа "жизненного цикла" хищения идентификационных данных (попытка получить персональную информацию жертвы; неправомерное использование полученной информации; и использование выгод от преступления, пока жертва не осознает причиненного ущерба). Сама стратегия направлена на развитие ключевых областей улучшения работы, включая следующее: профилактика (защита конфиденциальных данных и создание дополнительных препятствий для использования преступниками похищенных данных); реабилитация потерпевших (оказание потерпевшим помощи, с тем чтобы они смогли прийти в себя после преступления); сдерживающие меры в виде более строгого судебного преследования и наказания.

30. Что касается профилактических мер в публичном секторе, то г-н Раш упомянул практику сокращения необоснованного использования номеров социального страхования, а также образовательные программы для федеральных агентов по защите данных и обеспечению эффективного реагирования на неправомерное использование данных. Точно так же были определены решения для частного сектора, как, например, установление стандартов в области защиты данных и требований уведомлять о нарушениях, развитие системы всестороннего учета номеров социального страхования, используемых в частном секторе, повышение уровня образования в области защиты данных, расследование нарушений безопасности данных и проведение информационно-просветительских кампаний. Что касается реабилитации потерпевших, то здесь стратегия сконцентрирована на следующих приоритетных направлениях: подготовка сотрудников, оказывающих непосредственную помощь потерпевшим; индивидуальная помощь потерпевшим; внесение изменений в уголовное законодательство, касающееся реституции, для того чтобы обеспечить потерпевшим возмещение стоимостного эквивалента времени, потраченного в попытке прийти в себя от причиненного вреда; и оценка эффективности средств, имеющихся в распоряжении потерпевших. В области обеспечения соблюдения закона стратегия сконцентрирована в основном на координации и обмене информацией, в том числе посредством создания национального центра, использования одинаковой формы сообщения о преступлении и активизации обмена данными и информацией (в настоящее время около 40 штатов имеют свои собственные стандарты для уведомления о хищении идентификационных данных). Другие приоритетные направления деятельности в области обеспечения соблюдения закона включают более строгое судебное преследование в связи с совершением преступлений с использованием личных данных, а также координацию работы с зарубежными коллегами из правоохранительных органов наряду с учебными занятиями и последующими мерами по определению успеха правоохранительной деятельности.

31. Г-н Раш далее сообщил, что вызывает озабоченность и более активное участие организованных преступных группировок в преступлениях с использованием личных данных, и это также учитывается в стратегии. Одна из трудностей, возникших в этой связи, – это использование документов в целях идентификации, выходящих за рамки ее первоначальных задач. Поэтому важно понять, как действуют организованные преступные группировки, для того чтобы обеспечить принятие более адекватных мер. Важно также установить

контакты с частным сектором с целью разработки комплекса практических совместных мер реагирования.

32. В порядке развития стратегии США в 2008 году была создана Межведомственная рабочая группа по обеспечению соблюдения законов о хищении идентификационных данных для проведения ежемесячных заседаний, а также брифингов представителей исследовательских организаций из частного сектора. Была также создана Международная рабочая группа по преступлениям с использованием личных данных при участии Канады, Соединенного Королевства и Соединенных Штатов Америки. При этом учитывались и некоторые рекомендации группы ведущих экспертов. В целом, по оценке выступавшего, нынешняя ситуация в борьбе с преступлениями с использованием личных данных улучшилась после принятия вышеупомянутых программных мер, но пока все равно не является вполне удовлетворительной. Поэтому основополагающее значение имеет регулярная оценка проделанной работы.

33. Г-н Джон Ансуорт рассказал о работе Министерства внутренних дел Соединенного Королевства в отношении преступлений с использованием личных данных. Национальному бюро оперативной информации о мошенничестве было поручено обновить оценку, проведенную в 2010 году в области преступлений с использованием личных данных. Работа велась в сотрудничестве со всеми национальными правоохранительными органами, партнерами из частного сектора и департаментами Министерства внутренних дел. Сбор полной информации по соответствующим вопросам по-прежнему является достаточно сложной задачей, и поэтому важнейшее значение здесь имеет налаживание отношений с другими секторами. Хотя общественность все лучше осознает эту угрозу, многое еще предстоит сделать для организации защиты. Преступления с использованием личных данных также связаны с другими преступлениями, в том числе с организованной преступностью. Г-н Ансуорт сообщил, что, по оценкам, каждый год жертвами хищений личных данных становятся около 1,8 миллиона человек (один человек каждые 20 секунд). Однако о значительной части этих преступлений, похоже, не сообщается. Еще одним следствием является то, что из-за мошеннических действий около 2,5 млрд. фунтов стерлингов переплачивается в виде налоговых скидок.

34. Г-н Ансуорт подчеркнул, что правоохранительные органы часто концентрируются на конечном преступлении и, возможно, упускают возможность сосредоточиться непосредственно на преступлении, связанном с использованием личных данных, которое было совершено на более раннем этапе преступной деятельности. Министерство внутренних дел признает необходимость межсекторального подхода и рационализации деятельности в целях всестороннего охвата угроз, создаваемых этой формой преступности. В этом контексте Совет по осуществлению стратегии в отношении преступлений с использованием личных данных (SIB) разработал межсекторальную стратегию, которая направлена в том числе на решение следующих задач на разных уровнях: обеспечение надежности документов (расширение возможностей деловых кругов и публичного сектора для проверки и удостоверения подлинности идентификационных данных, будь то в режиме онлайн или лично); укрепление правоохранительных мер (эффективное

распределение ресурсов в целях пресечения преступной деятельности, связанной с изготовлением, хищением и распространением поддельных или присвоенных удостоверений личности); усиление работы по предупреждению преступности (предоставление информации о выявленных поддельных идентификационных данных публичному и частному секторам с целью предупреждения); и поощрение образовательных программ (распространение информации в целях расширения прав и возможностей физических и юридических лиц в деле своей собственной защиты). Эта стратегия находится под постоянным контролем, что позволяет обеспечить ее реализацию.

35. После представления материалов участники пришли к выводу, что наличие и осуществление национальных стратегий в области предупреждения преступлений с использованием личных данных и борьбы с ними могли бы играть важную роль в привлечении внимания и ресурсов и обеспечении их использования таким образом, чтобы эффективно координировать это с усилиями по борьбе с преступностью в целом, с другими задачами, представляющими общественный интерес, а также с деятельностью и интересами частного сектора. Такие национальные стратегии могли бы также играть заметную роль на международном уровне, внося ясность в политику, законодательство и стратегии каждой страны и формируя основу для обсуждений или переговоров относительно координации и сотрудничества между государствами-членами. Это особенно важно в связи с преступлениями с использованием личных данных ввиду широкого диапазона затронутых задач и интересов в сфере безопасности, экономики и личной жизни, а также того факта, что проблема эта сейчас возникает по большей части в режиме онлайн и в цифровых системах. Участники также согласились, что детали таких стратегий могут различаться в разных государствах-членах, но по меньшей мере перечень ключевых стратегических элементов мог бы стать той основой, которую каждое государство, возможно, пожелает принять во внимание при разработке такой стратегии.

36. В этой связи участники обсудили содержание проекта краткого наброска элементов для включения в национальные стратегии по предупреждению, расследованию преступлений с использованием личных данных и судебного преследования и наказания виновных в их совершении. Этот набросок был подготовлен Секретариатом на основе документа докладчика (см. пункт 27 выше) и результатов их обсуждения примеров национальной практики, упоминавшихся в рамках данного пункта повестки дня. Группа ведущих экспертов сделала ряд предложений по структуре и содержанию проекта наброска, который, как было в конечном итоге решено, прилагается к настоящему докладу (см. добавление II). Группа ведущих экспертов также решила, что документ, подготовленный докладчиком, должен быть дополнительно доработан и обновлен и представлен Комиссии на ее двадцать второй сессии как документ зала заседаний. Комиссия, возможно, пожелает рассмотреть как набросок, так и документ зала заседаний как руководство в работе и предложить далее государствам-членам представить Секретариату ответы, отражающие их собственное видение вопроса о национальной стратегии борьбы с преступлениями с использованием личных данных.

D. Работа других международных и межправительственных организаций

37. Г-н Кристофер Хорнек и г-н Поль Пикар рассказали о деятельность ОБСЕ в области управления использованием идентификационных данных. Различные подразделения ОБСЕ занимаются разными аспектами этой проблемы: например, Бюро по демократическим институтам и правам человека занимается вопросами миграции (запись актов гражданского состояния и регистрация населения) или выборов (базы данных по избирателям), а Отдел по экономическим и экологическим вопросам – вопросами эффективного управления и регулирования миграции. Однако основную работу в данной области ведет Департамент по транснациональным угрозам, в частности его Сектор по борьбе с терроризмом. Работа ОБСЕ сосредоточена на практических аспектах, связанных с выдачей документов, их обработкой, улучшением управления использованием идентификационных данных, содействием повышению качества документов, включая содействие внедрению стандартов Международной организации гражданской авиации (ИКАО), и выявлением фальшивых документов в ходе пограничного контроля.

38. ОБСЕ также участвует в различных рабочих группах, занимающихся этой тематикой, и с 2003 года осуществила более 55 проектов, причем некоторые из них в сотрудничестве с ИКАО, Интерполом, Международной организацией по миграции (МОМ), Европейским союзом и Международной организацией по стандартизации (ИСО). ОБСЕ реализует долгосрочные проекты в Республике Молдова, Таджикистане, Узбекистане и Кыргызстане. Кроме того, была представлена краткая информация по справочнику открытых ключей ИКАО. Доступ к нему можно получить бесплатно в Интернете, но за загрузку документов придется платить. В заключение было отмечено, что проблемы все еще сохраняются, и их необходимо решать в целях улучшения управления идентификационными данными и ускорения процесса пограничного контроля.

39. Г-н Чже Сун Ли рассказал о работе Комиссии Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ) в области управления использованием идентификационных данных. ЮНСИТРАЛ была пионером в разработке международных стандартов в области электронной торговли, которые оказали влияние на национальное законодательство стран. В этой связи в 2008 году были приняты показатели по мошенничеству в коммерческом секторе. С расширением использования электронных сообщений в международной торговле почти все рабочие группы ЮНСИТРАЛ затрагивают связанные с этим вопросы при обсуждении соответствующих тем. Они делают акцент на тех аспектах управления идентификационными данными, которые имеют отношение к упрощению процедур торговли, однако специального документа по этому вопросу не принято. Рабочая группа IV по электронной торговле на своем совещании в октябре 2012 года рассмотрела вопросы управления идентификационными данными. Группа разработала типовой закон об электронной торговле, в котором содержится общая схема управления идентификационными данными, а также типовое законодательство, касающееся электронной подписи. Группа также затронула такие вопросы, как концепция системы управления идентификационными данными, ее коммерческая модель, процессы и основные действующие лица, а также

потенциальные выгоды. Такие системы управления идентификационными данными предназначены для идентификации и удостоверения подлинности пользователей, желающих получить доступ к услугам, и являются своего рода инструментом укрепления доверия к электронной торговле. В 2011 году был проведен коллоквиум, на котором был достигнут широкий консенсус относительно важности вопросов управления идентификационными данными для содействия трансграничным электронным сделкам. Было высказано мнение, что ЮНСИТРАЛ, вероятно, лучше всего подходит для работы над транснациональными правовыми аспектами управления идентификационными данными. Такая работа позволила бы также дополнительно прояснить сферу применения положений о юридической силе подписи, которые содержатся в существующих текстах ЮНСИТРАЛ, и облегчила бы решение вопросов управления идентификационными данными в контексте других тем, представляющих потенциальный интерес для ЮНСИТРАЛ. Поэтому Рабочей группе IV было поручено работать над вопросом управления идентификационными данными в области электронных передаваемых записей. Следует отметить, что Целевая группа по правовым аспектам управления идентификационными данными Американской ассоциации адвокатов представила для возможного обсуждения в рабочей группе документ с общим обзором использования идентификационных данных, его роли в электронной торговле и соответствующих правовых вопросов, а также существующих барьеров.

40. ЮНСИТРАЛ в настоящее время занимается отслеживанием различных инициатив в отношении управления идентификационными данными, для того чтобы лучше определить условия возможного будущего мандата рабочей группы. ЮНСИТРАЛ также сотрудничает с Европейским союзом в работе над предложенными "Положениями об оказании электронных услуг по идентификации и обеспечению надежности электронных операций на внутреннем рынке". Другая деятельность включает создание европейской функционально совместимой платформы для электронной идентификации (Secure Identity Across Borders Linked); сотрудничество с МОМ в вопросах организации пограничного контроля; сотрудничество с Организацией по развитию стандартов структурированной информации в решении проблемы торговли и идентификационных данных; и создание общеевропейской интерактивной программы по публичным закупкам.

E. Техническая помощь – области для принятия мер: законодательные меры, управление идентификационными данными и предупреждение преступлений с использованием личных данных

41. Группа ведущих экспертов напомнила о предыдущих мандатах, предусматривавших оказание технической помощи в борьбе с преступлениями с использованием личных данных (см. пункты 7-8 резолюции 2009/22 ЭКОСОС), и подвела итоги соответствующей работы, осуществлявшейся в соответствии с ее указаниями и рекомендациями. В этом контексте было упомянуто об основных итогах работы, проделанной группой ведущих экспертов в прошлом, как, например, о подготовке исследовательских

документов по подходам к проблеме криминализации, вопросам виктимизации и партнерским отношениям между публичным и частным секторами. Особо был также упомянут Справочник по преступлениям с использованием личных данных, который содержит всеобъемлющее руководство для практических работников по международному сотрудничеству в борьбе конкретно с преступлениями с использованием личных данных (см. выше пункт 2).

42. При дальнейшем обсуждении вопросов технической помощи группа ведущих экспертов подтвердила, что бóльшая часть будущей работы в этой области будет зависеть от наличия ресурсов, необходимых как для подготовки материалов по технической помощи, так и для фактического осуществления проектов. Группа ведущих экспертов также согласилась, что полезно было бы наладить совместную деятельность и взаимодействие между публичным и частным секторами. Благодатной почвой для совместных инициатив могло бы стать предупреждение преступлений с использованием личных данных во всех ее формах, а именно социальная профилактика (образование, повышение информированности), ситуационная профилактика (в отношении лиц, сталкивающихся с конкретными рисками виктимизации, или подготовка тех, кто занимаются выявлением преступлений с использованием личных данных) и техническая профилактика (разработка технических мер безопасности для обеспечения надежности документов).

43. Кроме того, группа ведущих экспертов согласилась с необходимостью придерживаться целенаправленного подхода и определить приоритетные области для принятия эффективных мер по оказанию технической помощи. Первостепенное значение и приоритет, как все единодушно согласились, имеют законодательные меры. В связи с этим было признано, что техническую помощь следует в первую очередь ориентировать на создание отвечающей необходимым требованиям соответствующей нормативно-правовой базы для борьбы с преступлениями с использованием личных данных. Цель должна заключаться в оказании государствам-членам помощи в разработке новой или обновлении существующей базы по преступлениям, с тем чтобы реагировать на неправомерное использование и фальсификацию личных данных в преступных целях, а также в создании необходимых правовых механизмов и инструментов для обеспечения эффективного уголовного преследования и расследования преступлений с использованием личных данных.

44. В свете вышеизложенного было решено, что разработка типового законодательства по преступлениям с использованием личных данных могло бы принести дополнительную пользу государствам-членам, которые хотели бы руководствоваться сводом типовых положений в структурной организации эффективных правовых мер. До сведения группы ведущих экспертов был доведен образец, подготовленный профессором Герке, с тем чтобы ознакомить с контрольным перечнем вопросов, которые следует рассмотреть на предмет возможного включения в типовое законодательство. Профессор Герке подтвердил, что невозможно эффективно установить уголовную ответственность собственно за нарушения, связанные с использованием личных данных, без единой системы управления идентификационными данными. Поэтому предлагаемая схема типового законодательства по преступлениями с использованием личных данных (см. добавление I) включает также аспекты административного характера, которые связаны с программой

работы в области управления идентификационными данными. Таким образом, государства-члены, которые желают руководствоваться типовым законодательством, основанным на этой схеме, могут сами определить сферу применения нормативно-правовой базы с учетом того, что аспекты управления идентификационными данными могут также рассматриваться в более широком контексте национальной стратегии в отношении преступлений, связанных с личными данными.

F. Вовлечение частного сектора в разработку и осуществление программ технической помощи: партнерские отношения между публичным и частным секторами

45. Представители Британской ассоциации банкиров (БАБ) рассказали о работе Ассоциации по борьбе с финансовыми преступлениями, а также об их нынешнем сотрудничестве с публичным сектором. БАБ представляет 200 финансовых учреждений, действующих в 60 странах мира. В рамках этой деятельности БАБ организовала работу семи комитетов по финансовым преступлениям, один из которых занимается конкретно вопросами мошенничества. Эти комитеты являются директивными органами и дают, например, рекомендации правительству по стратегическим вопросам. БАБ также доводит до сведения правительства мнения и проблемы банковского сектора, например в связи с обменом – в рамках банковского сектора – информацией о подозрительных операциях, или те, что связаны с вызовами, обусловленными ростом международных операций их клиентов. О степени приверженности банковского сектора делу борьбы с финансовыми преступлениями свидетельствуют значительные средства, которые он выделяет на эти цели, его стремление обеспечить безопасность своих систем и прием на работу квалифицированных работников, многие из которых являются бывшими сотрудниками правоохранительных органов.

46. Представители БАБ особо отметили важность взаимодействия между частным и публичным секторами и сотрудничества членов Ассоциации с правоохранительными органами, в том числе путем предоставления информации о путях выявления подозрительных операций. Кроме того, БАБ является одним из элементов национальной стратегии борьбы с мошенничеством и принимает активное участие в других совместных инициативах публичного и частного секторов, как, например, информационно-просветительские кампании в Интернете. Такое взаимодействие имеет основополагающее значение ввиду того факта, что финансовые преступления постоянно эволюционируют и требуют общих усилий обоих секторов, направленных на то, чтобы должным образом реагировать на эти новые вызовы. Точно так же сотрудничество может быть весьма полезным в борьбе с отмыванием денег, поскольку это одна из основных проблем, с которыми сталкиваются члены БАБ. Было отмечено, что частный сектор может внести ценный вклад в дальнейшее создание законодательных и политических условий для борьбы с финансовыми преступлениями и отмыванием денег. Отмечалась также роль международного сообщества в борьбе с финансовыми преступлениями.

47. Представители БАБ также подчеркнули, что одним из ключевых факторов является просвещение общественности. Судя по их опыту, системы банков хорошо защищены и не подвергаются прямым атакам хакеров. Однако сообщения клиентов, отправляемые по электронной почте, могут быть взломаны, и в результате этого в большинстве случаев преступники имеют возможность получить доступ к банковским учетным записям законным способом. Они также подчеркнули, что банковское сообщество неоднородно. Например, при решении проблемы преступлений с использованием личных данных в сфере банковских услуг, связанных с инвестициями, и банковских услуг для физических лиц преследуются различные цели.

48. Отвечая на вопрос, заданный г-ном Жилберту Мартиншем ди Алмейдой относительно новых потенциальных рисков, связанных с расширяющимся использованием новых систем, как, например, платежи, совершаемые с помощью мобильной связи, г-н Мэтью Аллен подчеркнул необходимость учитывать потенциальные слабые стороны в других секторах, таких как розничная торговля или сектор телекоммуникаций, при оценке рисков, связанных с финансовыми преступлениями. Однако не все новые продукты создают одинаковые риски; в этой связи проблемы возникают вследствие все более широкого использования новых технологий, например, совершения платежей с помощью мобильных телефонов в развивающихся странах. Международное сообщество могло бы сыграть свою роль в решении и этой проблемы.

49. Г-н Себастьян Сейар рассказал о работе RESOCOM и Reso-клуба. RESOCOM специализируется на борьбе с преступлениями с использованием личных данных и создает веб-службы для проверки подлинности документов, удостоверяющих личность, и паспортов всех стран. Как сообщается, в 2011 году была произведена проверка более 2 миллионов документов.

50. RESOCOM является членом-основателем Reso-клуба, цель которого – расширять контакты и обмены передовым опытом между специалистами из публичного и частного секторов в отношении борьбы с преступлениями с использованием личных данных. Ассоциация Reso-клубов организует в октябре 2013 года в Париже свой третий европейский форум по борьбе с преступлениями с использованием личных данных и документов, удостоверяющих личность. Ассоциация также стремится развивать проекты по оказанию помощи жертвам преступлений с использованием личных данных.

51. На основании вышеуказанных материалов группа ведущих экспертов обсудила вопрос о разработке описательного документа, содержащего изложение и обобщение добровольного опыта в налаживании партнерских отношений между публичным и частным секторами на международном уровне как одного из средств, иллюстрирующих их значение. Группа ведущих экспертов санкционировала проведение дальнейших мероприятий по подготовке подборки примеров успешного осуществления партнерства между публичным и частным секторами в целях борьбы с преступлениями с использованием личных данных в различных географических регионах. Документ с кратким описанием каждого случая (выгоды, представленные в количественном выражении и в цифровом виде) без включения аргументированного/редакционного анализа будет представлен Комиссии по

предупреждению преступности и уголовному правосудию на ее двадцать второй сессии в качестве документа зала заседаний.

52. Группа ведущих экспертов уполномочила далее Секретариат запросить у организаций частного сектора, представленных на совещании через посредство БАБ и Reso-клуба, более подробную информацию, включая примеры из практики, по следующим вопросам: последствия преступлений с использованием личных данных для этих организаций; подготовка любых количественных (цифры) и/или качественных данных, включая оценки и мнения относительно некоторых путей решения проблем, связанных с такой формой преступности; виды инициатив/мер, которые были предприняты субъектами частного сектора для расширения работы по предупреждению преступлений с использованием личных данных; меры, которые были приняты для защиты потребителей от виктимизации; виды осуществляемой подготовки, если таковая организована, для сотрудников и должностных лиц, на которых возложена задача выявления преступлений с использованием личных данных; практическая выгода от укрепления партнерских связей между публичным и частным секторами в плане предотвращения преступлений с использованием личных данных и борьбы с ними; и области, в которых взаимодействие между государственными органами и финансовыми учреждениями/другими организациями частного сектора может дать ощутимые плоды и эффективные результаты.

G. Представление показательных примеров образовательных проектов, включающих элементы профилактики и выявления преступлений с использованием личных данных

53. Профессор Никос Пассас при поддержке своих коллег из Северо-Восточного университета в Бостоне, США, которые участвовали в работе совещания благодаря организации телеконференции, проинформировал группу ведущих экспертов о ряде проектов, разработанных – или находящихся в стадии разработки – в университете и включающих аспекты, связанные с профилактикой и выявлением преступлений с использованием личных данных. Первый проект чем-то напоминал секретную операцию в области киберпреступности и преследовал цель произвести вброс информации в преступную сеть, чтобы понять, как функционирует подпольная кибер-экономика. Второй проект под названием "Mediascan" предназначен для использования банками и финансовыми учреждениями и направлен на выявление и отслеживание подозрительных и необычных сделок, которые часто связаны с неправомерным использованием идентификационной информации. Третий проект посвящен анализу практики, связанной с сокрытием или неправомерным использованием идентификационных данных в контексте неформальных платежей и отмывания денег с помощью торговли.

H. Прочие вопросы

54. Г-н Кнопейс представил так называемый проект "Лояльность" ("Fidelity") – проект Европейского союза, направленный на анализ недостатков и уязвимых мест, возникающих в течение срока службы электронного

паспорта, а также разработку технических решений и рекомендаций по их преодолению. В этом четырехлетнем проекте участвуют 19 партнеров (МСП, представители отрасли, конечные пользователи, ученые), и он сконцентрирован на SWOT-анализе (выявление и структурирование сильных и слабых сторон, а также потенциальных возможностей и угроз) в течение срока службы электронных паспортов. Г-н Кнопейс проинформировал о различных проблемах, возникающих на тех или иных этапах срока службы электронных паспортов, как, например, те, что встречаются в процессе выдачи (надежность свидетельства о рождении и другие доказательства подлинности), или те, что связаны с аннулированием и уничтожением интегральных микросхем. Говорилось об организации работы со свидетельствами, обеспечении защиты персональных данных на протяжении всего процесса, а также о проверке качества биометрических данных. Выступающий отметил, что возникла насущная необходимость установить минимальные международные стандарты в отношении свидетельств о рождении (см. ниже) и других доказательств подлинности в целях повышения степени обеспечения неприкосновенности документов, удостоверяющих личность.

55. Кроме того, г-н Кнопейс выступил с докладом по вопросам обеспечения надежности, возникающим в связи с документами, которые выдаются родителям и являются первым идентификационным свидетельством при рождении. Эти документы, выдаваемые с ведома государственных органов, часто вызывают вопросы в плане надежности, поскольку никаких стандартов или критериев в отношении них не установлено. Докладчик особо отметил отсутствие международных стандартов и информации о документах, выдаваемых родителям в других странах. В настоящее время нет никакой базы данных по таким документам, в которой государственные органы могли бы найти информацию об используемой модели, и познания в этой области ограничены. Поэтому существует опасность использования поддельных выдаваемых родителям документов для получения имеющей законную силу защищенной идентификационной карты или паспорта.

56. В этом же контексте г-н Кнопейс представил и рабочее определение управления идентификационными данными как системы, включающей видение, политику и средства для управления идентификационными данными всех граждан, осуществляемого государственными органами. В связи с этим группе ведущих экспертов была представлена таблица по инфраструктуре идентификационной информации с четырьмя этапами всего срока существования документа (изготовление, использование и одновременный контроль, окончание использования). По каждому из этих этапов были даны технические разъяснения, касающиеся вопросов регистрации, задействованных процессов и необходимого опыта.

IV. Выводы и рекомендации в отношении дальнейших действий

57. На последнем заседании совещания 18 января 2013 года Председатель группы ведущих экспертов подвел основные итоги обсуждения следующим образом:

a) разработка схемы для типового законодательства по преступлениям с использованием личных данных; и

b) подготовка контрольного перечня стратегических элементов в разработке национальных стратегий в области предупреждения, расследования преступлений с использованием личных данных и судебного преследования и наказания виновных в их совершении.

Оба этих результата приводятся в добавлениях к настоящему докладу.

58. Председатель также отметил, что группа ведущих экспертов предложила конкретные рамки для дальнейших действий, в частности на период после завершения шестого совещания группы ведущих экспертов и до двадцать третьей сессии Комиссии. В этой связи группа ведущих экспертов сделала следующие рекомендации в отношении последующей деятельности:

a) обновить описательный документ по разработке рамок с основными элементами национальной стратегии в области предупреждения, расследования преступлений с использованием личных данных и судебного преследования и наказания виновных в их совершении; и представить затем этот документ на рассмотрение Комиссии на ее двадцать второй сессии в качестве документа зала заседаний;

b) разработать описательный документ с подборкой примеров успешного партнерства между публичным и частным секторами в борьбе с преступлениями с использованием личных данных в различных географических регионах; и представить затем этот документ на рассмотрение Комиссии на ее двадцать второй сессии в качестве документа зала заседаний;

c) собрать информацию о преступлениях с использованием личных данных у организаций частного сектора в соответствии с приведенными выше указаниями и рекомендациями (см. пункт 52);

d) разработать типовое законодательство по преступлениям с использованием личных данных с учетом схемы, приведенной в добавлении к настоящему докладу. Что касается используемой методологии, то здесь наиболее подходящим способом достижения этой цели была сочтена инициатива Секретариата создать, при условии наличия внебюджетных средств, специальную группу экспертов для решения этой задачи; и

e) запросить у государств-членов дополнительную информацию о разработке и осуществлении национальных стратегий или программ по предупреждению преступлений с использованием личных данных и борьбе с ними.

Добавление I

Схема типового законодательства по преступлениям с использованием личных данных

1. Определение

В этом разделе можно дать определения наиболее важных терминов. Помимо "личных данных", "средств идентификации", "владения", "использования" и "передачи" раздел определений мог бы также содержать определения технических терминов.

2. Уголовные материально-правовые положения

Типовой закон мог бы содержать уголовные материально-правовые положения в отношении преступлений с использованием личных данных, совершаемых в режиме онлайн и офлайн (хищение личных данных/мошенничество с идентификационными данными). Для конкретных преступлений можно было бы предусмотреть особые положения или отягчающие обстоятельства (например, подделка кодов доступа к военному имуществу). Типовой закон мог бы также содержать положения уголовного права, предусматривающие уголовную ответственность за подготовительные действия, такие как изготовление, продажа, ввоз, вывоз или хранение средств, используемых для изготовления поддельных паспортов.

3. Процессуально-правовые положения

Теоретически типовой закон мог бы содержать целый ряд процессуально-правовых положений, которые позволили бы стране, не имеющей надлежащего законодательства по борьбе с киберпреступностью, эффективно бороться с преступлениями с использованием личных данных, совершаемыми в режиме онлайн. Однако здесь может возникнуть дублирование с другими инициативами, что может привести к коллизиям. Поэтому было бы предпочтительнее сосредоточиться исключительно на вопросах, связанных с личными данными. Одним из таких вопросов, например, могло бы стать замораживание, арест и конфискация активов и/или информации, связанной с идентификационными данными.

4. Электронные доказательства

Некоторые положения могли бы касаться приемлемости конкретных доказательств совершения преступлений с использованием личных данных. Можно было бы также рассмотреть обязательство передавать записи потерпевшему.

5. Неотложные вопросы

Типовое законодательство могло бы содержать положения, позволяющие в срочном порядке принимать меры по текущим делам, если поступает сообщение о преступлении с использованием личных данных. Одним из примеров могло бы быть "замораживание в целях обеспечения безопасности" (см. выше в разделе "Процессуально-правовые положения").

6. Обязательства по представлению информации и уведомлений

Типовое законодательство могло бы содержать положения, устанавливающие для компаний, которые стали жертвами преступлений с использованием личных данных (в связи с данными о клиентах), обязанность сообщать об этом правоохранительным органам. Кроме того, типовое законодательство могло бы предусматривать обязательства в отношении уведомления, требующие от компаний уведомлять клиента, если его данные были получены незаконным путем. Типовое законодательство могло бы также содержать положения, устанавливающие механизмы представления информации (например, веб-сайты для жалоб).

7. Защита информации, связанной с личными данными

Типовое законодательство могло бы предусматривать запрет на использование определенной идентификационной информации, а также обязательства хранить такую информацию с соблюдением определенных стандартов защиты (например, шифрование) и технических стандартов в отношении удаления/уничтожения идентификационной информации.

8. Статистика

Типовой закон мог бы содержать положения, устанавливающие определенные требования в отношении представления информации для сбора статистических данных для полицейской статистики.

Добавление II

Контрольный перечень стратегических элементов в разработке национальных стратегий в области предупреждения, расследования преступлений с использованием личных данных и судебного преследования и наказания виновных в их совершении

В этом контрольном перечне указаны заинтересованные стороны, а также основные элементы и процессы, которые каждое государство, возможно, пожелает использовать при разработке национальных стратегий в области предупреждения, расследования преступлений с использованием личных данных и судебного преследования и наказания виновных в их совершении.

A. Возможные заинтересованные стороны или участники осуществления национальной стратегии

- публичный сектор (публичные органы, отвечающие за инфраструктуру, документы или системы, связанные с идентификационными данными, учреждения, отвечающие за политику и законодательство в более общем плане, органы, отвечающие за расследование, предупреждение преступлений, судебное преследование за их совершение и т.д.);
- частный сектор (например, представители секторов, занимающихся финансами, розничной торговлей и информационными технологиями);
- региональные и международные организации.

B. Основные элементы национальной стратегии

- оценка угроз – понимание характера и масштабов проблемы/ситуации;
- сбор, распространение и анализ соответствующей информации о проблеме;
- установление приоритетов и координация между публичным и частным секторами;
- законодательные элементы – криминализация, правоохранительная деятельность, международное сотрудничество, а также меры неуголовного/административного характера;
- следственный и правоохранительный потенциал;
- элементы для поддержки оперативного вмешательства в целях пресечения и прекращения работы существующих схем совершения преступлений с использованием личных данных;
- элементы, связанные с предупреждением преступности: социальная профилактика (образовательные программы, повышение информированности); ситуационная профилактика (информация для конкретных групп, либо потому что они сталкиваются с конкретными рисками виктимизации, либо потому что они работают в таких местах, где они могут выявлять и пресекать преступления с использованием

личных данных); техническая профилактика (меры безопасности для обеспечения неприкосновенности документов и систем);

- помощь потерпевшим;
- профессиональная подготовка следователей, сотрудников правоохранительных органов и других соответствующих работников и должностных лиц и представителей частного сектора;
- сотрудничество между публичным и частным секторами в осуществлении стратегии.

C. Процессы в рамках разработки и осуществления национальной стратегии

- выделение необходимых ресурсов для осуществления;
- проведение предварительных консультаций на всех уровнях правительственного сектора, а также с частным сектором;
- создание рабочих механизмов вертикальной координации (особенно в федеративных государствах);
- проведение консультаций или осуществление координации с международными заинтересованными сторонами, где это уместно;
- обеспечение постоянных консультаций между заинтересованными сторонами;
- обзор прогресса и устойчивости в осуществлении стратегии.